
Nortel Communication Server 1000

Nortel Communication Server 1000 Release 4.5

Converging the Data Network with VoIP

Document Number: 553-3001-160

Document Release: Standard 5.00

Date: July 2006

Copyright © 2006 Nortel Networks. All rights reserved.

Produced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Revision history

July 2006	Standard 5.00. This document is up-issued for changes in technical content.
March 2006	Standard 4.00. This document is up-issued for CR Q01286628, clarifying Network Diagnostic Utilities CLI commands.
August 2005	Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.
September 2004	Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.
October 2003	Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: Data Networking Guidelines (553-3023-103).

Contents

About this document	11
Subject	11
Applicable systems	11
Intended audience	13
Conventions	13
Related information	14
Overview	17
Contents	17
Introduction	17
Network convergence	20
Network design	21
Quality of Service	22
Network performance measurement and monitoring	24
Available tools	25
Achieving satisfactory voice quality	26
Network design assessment	27
Contents	27
Introduction	28
Network modeling	28
LAN and WAN platforms	33
Protocols in use	36

Link speeds	38
Link types	39
Link utilization assessment	40
Traffic flows in the network	42
Service level agreements	44
Summary	45
QoS mechanisms	47
Contents	47
Introduction	48
The QoS process	53
WAN QoS mechanisms	57
Layer 2 (Ethernet) QoS	65
Layer 3 QoS	72
Layer 4 (TCP/IP) classification	80
Policy management	81
Bandwidth Management	82
Network performance measurement	99
Contents	99
Introduction	100
Network performance measurement tools	108
Network availability	109
Bandwidth	110
Delay	126
Jitter	138
Packet loss	143
Network delay and packet loss evaluation example	147
Estimate voice quality	148
Does the intranet provide expected voice quality?	154

Configuration of the DHCP server	157
Contents	157
Overview	157
IP Phones	158
Configuring the DHCP server to support full DHCP mode	159
Server LAN design	169
Contents	169
Introduction	170
Ethernet requirements	181
IP address requirements	188
Guidelines for configuring a routable ELAN subnet	197
Redundant LAN design	197
Distributed IP Expansion Media Gateway requirements	203
Distributed Media Gateway 1000E	208
Campus-distributed Media Gateway enhancements	209
Sample system layout	211
Operating the VoIP network	221
Contents	221
System management	221
Network monitoring	223
Network Management	251
Appendix A: Subnet mask conversion from CIDR to dotted decimal format	255
Appendix B: Port number tables	257
Contents	257
Introduction	257

Appendix C: DHCP supplemental information ..	279
Contents	279
Introduction to DHCP	279
IP acquisition sequence	284
IP Phone support for DHCP	288
Appendix D: Setup and configuration of DHCP servers	297
Contents	297
Install a Windows NT 4 or Windows 2000 server	297
Configure a Windows NT 4 server with DHCP	298
Configure a Windows 2000 server with DHCP	301
Install ISC's DHCP Server	307
Configure ISC's DHCP Server	308
Install and configure a Solaris 2 server	312
List of terms	315

List of Procedures

Procedure 1	
Assessing link utilization	41
Procedure 2	
Configuring 802.1p priority bits in Element Manager	68
Procedure 3	
Calculating bandwidth amount for bandwidth zones table	94
Procedure 4	
Determining intrazone bandwidth	94
Procedure 5	
Evaluating network performance – overview	102
Procedure 6	
Calculating LAN traffic	113
Procedure 7	
Calculating WAN traffic	115
Procedure 8	
Determining network requirements – overview	119
Procedure 9	
Converting a subnet mask from CIDR format to dotted decimal format	255

Procedure 10	
Launching the DHCP Manager In Windows NT 4	298
Procedure 11	
Launching the DHCP Manager in Windows 2000	301
Procedure 12	
Configuring ISC's DHCP server	309
Procedure 13	
Configuring a Solaris 2 server	312
Procedure 14	
Configuring Solaris 2 to work with IP Phones	313

About this document

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

Subject

The purpose of this document is to provide direction in ensuring that the data network has been properly provisioned to support IP Telephony services.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Note: When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.5 software and configured to include a Signaling Server, they become CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

Table 1
Meridian 1 systems to CS 1000M systems

This Meridian 1 system...	Maps to this CS 1000M system
Meridian 1 PBX 11C Chassis	CS 1000M Chassis
Meridian 1 PBX 11C Cabinet	CS 1000M Cabinet
Meridian 1 PBX 51C	CS 1000M Half Group
Meridian 1 PBX 61C	CS 1000M Single Group
Meridian 1 PBX 81	CS 1000M Multi Group
Meridian 1 PBX 81C	CS 1000M Multi Group

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)

- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)
- *Communication Server 1000E: Upgrade Procedures* (553-3041-258)

Intended audience

This document is intended for network deployment personnel responsible for ensuring that the data network has been properly provisioned to support IP Telephony services.

This document assumes that the reader understands general data networking technology and has a fundamental understanding of IP networking technologies and protocols.

Conventions

Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as "Small System":

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as "Large System":

- Communication Server 1000M Half Group (CS 1000M HG)

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

Related information

This section lists information sources that relate to this document.

NTPs

The following NTPs are referenced in this document:

- *Main Office Configuration for the Survivable Remote Gateway 50: Configuration Guide* (553-3001-207)
- *Signaling Server: Installation and Configuration* (553-3001-212)
- *IP Peer Networking: Installation and Configuration* (553-3001-213)
- *Branch Office: Installation and Configuration* (553-3001-214)
- *Optivity Telephony Manager: Installation and Configuration* (553-3001-230)
- *Communication Server 1000: System Redundancy* (553-3001-307)
- *Software Input/Output: Administration* (553-3001-311)
- *Emergency Services Access: Description and Administration* (553-3001-313)
- *Optivity Telephony Manager: System Administration* (553-3001-330)
- *Element Manager: System Administration* (553-3001-332)
- *Call Detail Recording: Description and Formats* (553-3001-350)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *IP Phones: Description, Installation, and Operation* (553-3001-368)

- *Software Input/Output: System Messages* (553-3001-411)
- *Traffic Measurement: Formats and Output* (553-3001-450)
- *Software Input/Output: Maintenance* (553-3001-511)
- *Simple Network Management Protocol: Description and Maintenance* (553-3001-519)
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)

Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview

Contents

This section contains information on the following topics:

Introduction	17
Network convergence	20
Voice applications	21
Network design	21
Server LAN design	22
Configuring the DHCP server	22
Quality of Service	22
QoS versus bandwidth	23
Network performance measurement and monitoring	24
Application requirements	24
Available tools	25
Achieving satisfactory voice quality	26

Introduction

This NTP discusses a number of areas which you must address when building a converged multimedia network. These include:

- network design
- network performance
- Quality of Service (QoS)
- operations



WARNING

Before a CS 1000 system can be installed, a network assessment **must** be performed and the network must be VoIP-ready. See "Network design assessment" on page 27.

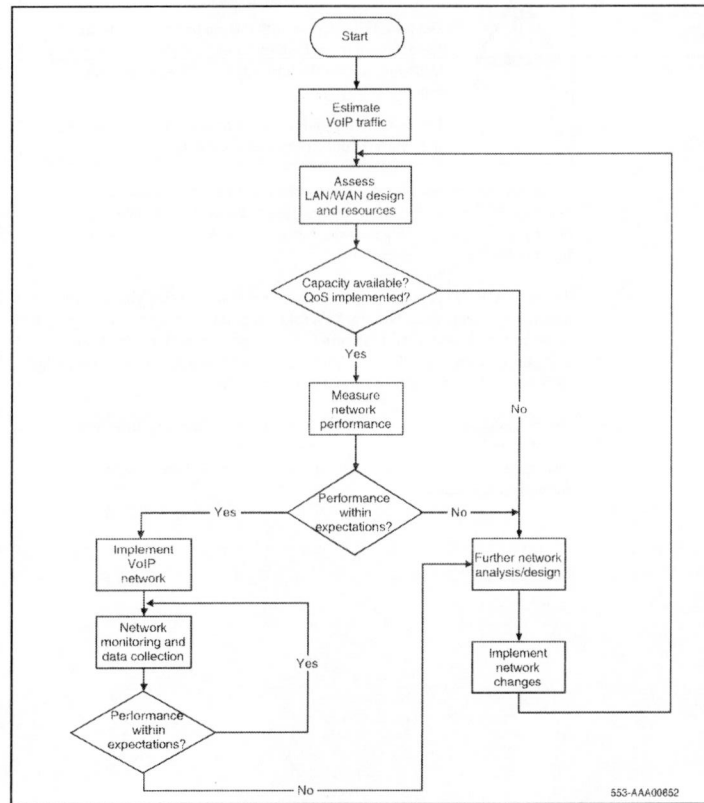
If the minimum VoIP network requirements are not met, the system does not operate properly.

Many considerations are important when creating and maintaining a converged network. It is important to gain a detailed understanding of the design of the existing data network before implementing a Voice over Internet Protocol (VoIP) network.

To create a VoIP-grade network, certain QoS standards for various basic network elements must be met. Several QoS parameters can be configured, measured, and monitored to determine if the desired service levels are provided and obtained. The mechanisms needed to design a robust, redundant QoS-managed VoIP network are described in this NTP.

Figure 1 on page 19 is a logical view of the steps necessary to assess a network for Voice over Internet Protocol (VoIP) readiness. Use this network assessment flow chart as a guideline for this NTP and the network engineering process.

Figure 1
Network assessment flow chart



Network convergence

Network convergence is the transport of all services over the same network structure. Previously, there were separate dedicated networks for different types of applications, such as voice, video, and data. Today, many of these applications are being merged into a single network to reduce operating costs and increase ease of operation.

A traditional enterprise can have the following network types:

- private Time Division Multiplexing (TDM)-based voice network
- IP network to the Internet
- Integrated Services Digital Network (ISDN) for video conferencing
- Systems Network Architecture (SNA) (an IBM computer network architecture)
- multi-protocol network, including such varied protocol types as Internetwork Packet Exchange (IPX) and AppleTalk

Many enterprises look to converged networks to achieve cost and operational efficiency. A converged network mixes different types of traffic, each with different requirements. This creates difficulties that must be addressed. When different types of applications had their own dedicated networks, QoS technology played a smaller role. Dedicated network traffic was similar in behavior, and the networks were fine-tuned to achieve the required behavior of the applications.

For example, the expectation for interactive voice is low packet loss and a minimal, fixed amount of delay. Data is sent in a steady stream, with samples transmitted at fixed time intervals. Such performance is obtained on a circuit-switched network. A best-effort data network has varying amounts of packet loss and variable delay usually caused by network congestion. A packet-based data network usually is the opposite of what is needed by a voice application.

Implementing QoS mechanisms helps to address this issue.

Voice applications

Voice applications originated on Public Switched Telephone Networks (PSTNs) and used circuit switching in the form of Time Division Multiplexing (TDM).

TDM has been engineered with very specific, predetermined behaviors to support real-time voice conversations. On a TDM network, bandwidth is guaranteed to be available for any voice call, therefore voice traffic experiences a low, fixed amount of delay, with essentially no loss.

IP networks do not guarantee that bandwidth will be available for voice calls unless QoS mechanisms are used to restrict delay and data loss to maintain acceptable user quality.

If a voice application is sent over a best-effort IP network (see page 22), the following can occur:

- Voice packets experience variable, unpredictable amounts of delay.
- Voice packets are dropped when the network is congested.
- Voice packets can be reordered by the network if the packets arrive out of sequence.

QoS techniques can be applied to properly-engineered networks to support VoIP with acceptable, consistent, and predictable voice quality.

Network design

It is important to have a detailed understanding of the converged network design. This can be done by answering the following questions:

- Is a physical network diagram available for the data and voice network?
 - Is a logical diagram for both networks available? The logical diagram can be provided by the SNMP Network Management System (NMS).
- What Local Area Network (LAN)/Wide Area Network (WAN) platforms are currently installed?
 - Do the currently installed platforms support some form of QoS?

- What types of links are in use?
 - Point-to-Point Protocol (PPP)
 - Frame Relay (FR)
 - Asynchronous Transfer Mode (ATM)
- What protocols are in use? What routing protocols are in use?
- What link speeds are in use on the LAN? What link speeds are in use on the WAN?
- What is the current utilization of those links?
 - What are the peak delays on the WAN links?
 - What is the current delay and packet loss?
- What is the current flow of data and voice traffic?

For more information, refer to "Network design assessment" on page 27.

Server LAN design

Server LAN design for the system is discussed in "Server LAN design" on page 169. The topics covered include Layer 2 design, IP addressing, and server LAN redundancy.

Configuring the DHCP server

IP Phones 200x support automatic configuration using the Dynamic Host Configuration Protocol (DHCP). See "Configuration of the DHCP server" on page 157 for details on configuring the DHCP server.

Quality of Service

IP networks are inherently "best-effort networks." They treat all packets in the same manner. A best-effort network has no specified parameters. It does not guarantee how fast data is transmitted over a network, and has no assurances that the data will even be delivered at all.

Therefore, a means of providing guarantees is required. The purpose of Quality of Service (QoS) mechanisms is to guarantee that the network treats certain packets in a specified manner.

QoS mechanisms refer to packet tagging mechanisms and network architecture decisions on the TCP/IP network to expedite packet forwarding and delivery.

QoS is especially important for low-speed links, where the usual amount of bandwidth available is only several hundred kbps. For example, data traffic could easily use all of the bandwidth available on a link, thereby causing voice quality problems. QoS mechanisms can be used to guarantee that network bandwidth is available for voice traffic.

End-to-end QoS is required for IP Telephony applications to achieve good voice quality and is achieved by ensuring that the different parts of the network apply consistent treatment to the telephony packets.

Many of the available QoS mechanisms are described in "QoS mechanisms" on page 47.

QoS versus bandwidth

One approach to network engineering says that QoS is not needed; simply increasing bandwidth provides enough QoS for all applications. This theory also states that implementing QoS is complicated; adding bandwidth is easy. However, due to the bursty nature of IP network traffic, even very large amounts of bandwidth may not be enough to prevent congestion during a burst of traffic at a particular instance in time.

If all networks had infinite bandwidth available so that network congestion never occurred, QoS technology would not be needed. While having adequate bandwidth provisioned on the network is very important, over provisioning may not be very realistic; therefore, QoS mechanisms are needed.

Network performance measurement and monitoring

TCP/IP was originally designed to reliably send a packet to its destination. Little consideration was given to the length of time it took to get there. Today, IP networks transport data from many different application types. Many of these applications require minimal delay. Delay is the length of time needed for information to travel through a network. Significant delay can adversely affect end-user quality; and in some cases, the application does not function at all.

Networks now carry many different types of traffic. Each traffic type has unique requirements for the following QoS parameters:

- availability
- bandwidth
- delay
- jitter
- packet loss

These QoS parameters can be measured and monitored to determine if they meet desired service levels. Each of these elements are discussed in detail in "Network performance measurement" on page 99. "Operating the VoIP network" on page 221 also discuss the ongoing monitoring, management, and measurement of the network.

Application requirements

Table 2 on page 25 lists the various QoS performance parameters required by some common applications. If these parameters are mixed over a common-use IP network and QoS technologies are not used, the traffic can experience unpredictable behavior.

Table 2
Common application performance parameters

Application	Relative bandwidth demand	Sensitivity to		
		Delay	Jitter	Packet Loss
VoIP	Low	High	High	High
Video Conferencing	High	High	High	Med
Streaming Video on Demand	High	Med	Med	Med
Streaming Audio	Low	Med	Med	Med
Web browsing (eBusiness)	Med	Med	Low	High
E-mail	Low	Low	Low	High
File Transfer	Med	Low	Low	High

Available tools

Recommendation

Tools are available for almost every aspect of converged network engineering. Nortel strongly recommends the use of appropriate tools when performing network engineering.

For example:

- Multi-protocol network design assessment software is commonly available. These tools can analyze a network, highlight potential problems, and propose possible solutions.
- SNMP-based network management systems are available for network design assessment and monitoring.
- Graphical device configuration managers are available for almost all network switches available and can be integrated into SNMP network management systems.

- Policy managers are available for implementing end-to-end QoS policies.
- Network performance measurement tools are available for monitoring network jitter, delay, and packet loss.

All of these tools can be operated from a central location on the network. Using available tools can greatly simplify network engineering and operations, ultimately resulting in lower costs and higher quality services.

Some of the Nortel-recommended tools are highlighted throughout this document.

Nortel also offers professional Network Architecture and Design services. For more information, contact a Nortel sales representative.

Achieving satisfactory voice quality

A satisfactory level of perceived voice quality is achieved through the following:

- a properly-engineered network
- good network equipment and redundancy
- adequate bandwidth for peak usage
- use of QoS mechanisms
- ongoing monitoring and maintenance

If these elements are not present, VoIP performance suffers.

This document provides recommendations for the following:

- network design and configuration
- QoS mechanisms
- performance measurements
- operational monitoring and maintenance

Network design assessment

Contents

This section contains information on the following topics:	
Introduction	28
Network modeling	28
Physical and logical network diagrams	29
Sample IP network model	29
LAN and WAN platforms	33
Campus platforms	34
Supported QoS mechanisms	35
Bandwidth and data network switch efficiency	35
Security and QoS	36
Protocols in use	36
Routing protocols	36
Mixing protocols	37
Link speeds	38
Link types	39
Point-to-point links (PPP)	39
Frame Relay	39
Asynchronous Transfer Mode (ATM)	40
Virtual Private Network	40
Link utilization assessment	40
Assessing link utilization	41
Traffic flows in the network	42
Available traffic tools	43

Service level agreements	44
Summary	45

Introduction



WARNING

Before a CS 1000 system can be installed, a network assessment **must** be performed and the network must be VoIP-ready.

If the minimum VoIP network requirements are not met, the system does not operate properly.

It is important to gain a full understanding of the design of an existing data network before implementing a VoIP network. This section describes key issues to consider when creating a new converged voice and data network.

For example, it is very important to assess the network for such things as:

- the distribution of protocols in the network
- the level of QoS on the network
- the link speeds, link types, and link utilization
- the traffic flows in the network

Some of the tools used to assess the VoIP network are described, as well as examples of logical connection diagrams for small, medium, and large campus networks.

Network modeling

Network analysis can be difficult or time-consuming if the intranet and the CS 1000 system installation are large. Commercial network modeling tools can analyze "what-if" scenarios predicting the effect of topology, routing, and bandwidth changes to the network. These modeling tools work with an existing network management system to load current configuration, traffic, and policies into the modeling tool. Network modeling tools can help to

analyze and test the recommendations given in this document to predict how delay and error characteristics impact the network.

Physical and logical network diagrams

To determine VoIP readiness, diagrams of both the data and voice infrastructure (physical and logical) are required. These diagrams are valuable when determining the platforms deployed in the network as well as the logical design such as the IP addressing architecture, link speeds, and connectivity.

Note: Network diagrams are typically created using SNMP Network Management Systems (NMS). NMS provides graphical views from physical connections between LANs and WANs to the logical connections of a Virtual LAN (VLAN).

From a voice perspective, the numbering plan and Call Detail Record (CDR) help to determine calling patterns in a multi-site environment.

Knowledge of routing of circuit-switched trunking facilities helps to determine utilization and bandwidth requirements for a VoIP deployment.

Sample IP network model

The CS 1000 and Meridian 1 systems are VoIP servers suited for typical campus network designs.

In most cases, the system is connected logically to the server layer, as the server layer is engineered for high-availability and security.

Having a large amount of bandwidth available at the server level, though not required by the Call Server, also helps to ensure satisfactory VoIP QoS.

Nortel recommends QoS mechanisms for all layers to ensure that voice traffic obtains a level of service greater than the level of service for the best-effort data traffic.

Physical connectivity, VLANs, and subnets for the core server components are configured at the server layer, following existing server layer design and conforming to the core server configuration requirements.

Alternately, if campus-distributed Media Gateway systems are used, they are connected at the distribution layer. The core IP network can be configured with multiple VLANs and subnets to meet the core server configuration requirements.

The following are planned based on the access and distribution layers' configuration:

- VLANs
- subnets
- QoS mechanisms for the IP Phones such as DiffServ and 802.1Q

Typical network topology

Figure 2 provides a reference model for a campus network.

Figure 2
Campus network reference model

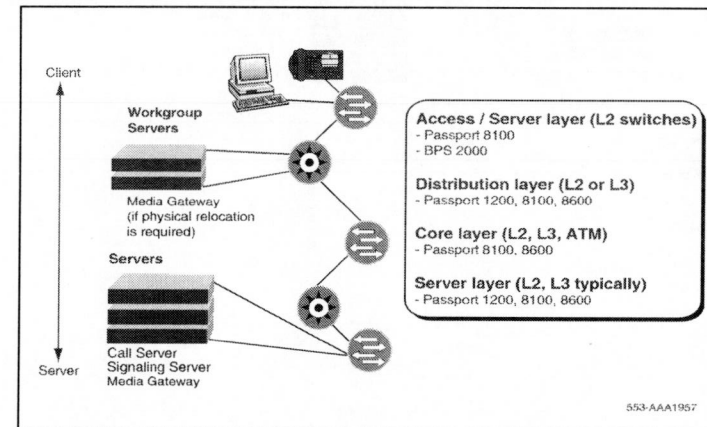


Figure 3, Figure 4 on page 32, and Figure 5 on page 33 show examples of logical connection diagrams for small, medium, and large campus networks. Other network designs can be used. The actual design that is implemented depends on many factors, including physical locations, size, and scalability.

Figure 3
Small campus network example

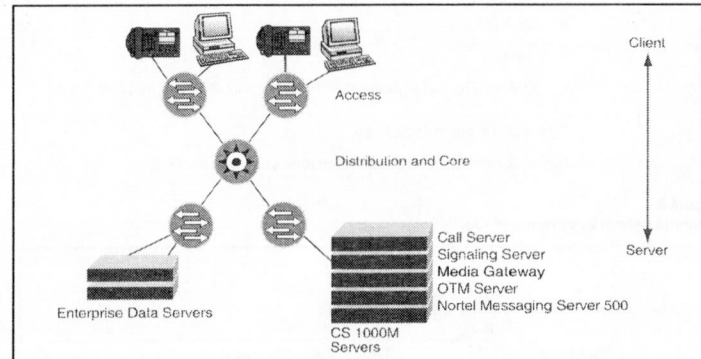


Figure 4
Mid-size campus network example

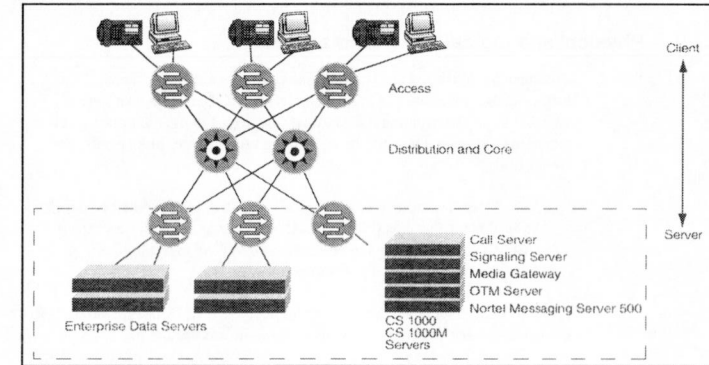
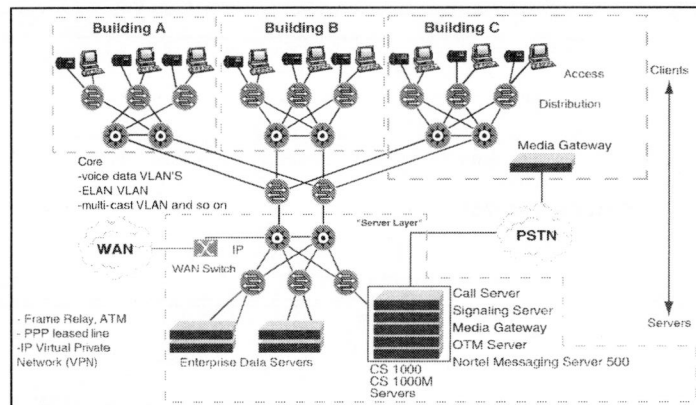


Figure 5
Large campus network example



Recommendation

Nortel strongly recommends that a network be designed to accommodate a larger VoIP deployment than will be installed, and that network administrators monitor network data traffic on a regular basis.

Network Modeling tools

Contact a Nortel sales representative if help is needed choosing a suitable Network Modeling solution.

LAN and WAN platforms

After determining the network topology, the next step is to evaluate the LAN and WAN platforms installed in the network.

If shared media is on the LAN, install Layer 2 switching as a minimum requirement. If there is a Layer 2 switched edge with a Layer 3 core, it is necessary to assess the bandwidth of the network.

The elements of a LAN/Campus network usually consist of the following:

- 100 Mbps bandwidth to the desktop
- high-performance closet switching
- devices such as the Business Policy Switch (BPS) connected to the core network
- multi-gigabit riser connections
- devices such as the Passport 8600 in the core

These networks require only the simplest QoS mechanisms. These types of devices can take advantage of DiffServ from end-to-end, if necessary.

If VoIP traffic travels on the WAN, high bandwidth can be achieved with networks connected through high-speed point-to-point Digital Signal Level 3 (DS3) links or through ATM/SONET services of Optical Carrier 3 (OC-3) and higher. All-optical networks with gigabit Ethernet also provide high-bandwidth transport.

Campus platforms

It is important to document the platforms used in the campus, and to document the following information for each switch:

- vendor
- switch model number
- hardware versions
- software versions

Typically, campus networks should be designed with high-bandwidth edge switches with multi-gigabit Ethernet connections to a switched Layer 3 IP network.

Riser access links and Layer 3 capacity are critical areas. If the desktop switching platform provides 24 connections at 100 Mbps and has only four 100 Mbps links, a significant bottleneck can occur at the riser. Serialization and queuing delays can become an issue that requires the application of QoS mechanisms such as 802.1Q/802.1p and/or DiffServ.

Migrating 100 Mbps riser links to Gigabit Ethernet is suggested.

**WARNING**

All VoIP servers and IP Phones must be connected to Layer 2 switches.

Shared-media hubs are not supported.
Shared-media hubs are low bandwidth devices and do not support QoS mechanisms.

Supported QoS mechanisms

To ensure consistent voice quality, some form of QoS must be supported on the platforms that transport VoIP. There are several ways to provide QoS, including the following:

- bandwidth management
- packet classification
- DiffServ
- fragmentation
- traffic shaping
- queuing mechanisms provided by the platform

If appropriate QoS mechanisms are not supported by the platform, an upgrade can be required.

Bandwidth and data network switch efficiency

It is important to note the maximum packets per second forwarding rates of the platforms. This determines the switch efficiency and the actual throughput the platform is capable of supporting.

Example

For 64-Byte packets and a 10-Mbps link, the maximum forwarding rate is 14 880 packets per second.

Bandwidth throughput is: $(64 \text{ B} / \text{P}) * (8 \text{ b} / \text{B}) * (14,880 \text{ P} / \text{S}) = 7.62 \text{ Mbps}$

A similar calculation is required for the WAN switches being used.

Note: Efficiency of an Ethernet switch is taken from the Performance Specifications section of the Ethernet switch manual.

Security and QoS

Consider the following security features:

- firewalls
- Network Address Translation (NAT) (See "NAT" on page 321.)
- Secure Virtual Private Network (VPN) access through Secure Internet Protocol (IPSec) encryption. (See "IPSec" on page 321.)

Routers might use NAT and IPSec for remote network users who connect to the network through the public Internet, using IPSec encryption. A firewall connection might also be in place. The network designer must consider the security policy in force and see if the ports required for VoIP can go through the firewall.

Protocols in use

When assessing the network for VoIP readiness, observe the distribution of protocols in the network, specifically on the WAN. Tools available for this task include Network Management Systems (NMS), which can poll devices through SNMP probes, RMON probes, or both, and analyze the results.

Routing protocols

It is important to note the routing protocols used within the network, as they can affect network availability.

LAN protocols

Routing protocols in the LAN must be considered when implementing VoIP.

WAN protocols

Routing protocols in the WAN can be very important when considering how VoIP calls will be routed and how quickly fail-over occurs. When planning a VoIP network, be aware of what situations trigger a routing table update with respect to the routing protocol. This helps when predicting what path a VoIP flow might take during a failure in the network.

Convergence

Convergence is the point where all internetworking devices have a common understanding of the routing topology. The time it takes a network to re-converge after a link failure must be considered, as the process might take several minutes depending on the network size and routing protocol in use.

Mixing protocols

VoIP performance can be impacted if a network is using multiple protocols on any particular segment.

For example, even with fragmentation implemented, if there are protocols in use other than IP, those protocols can maintain larger frame sizes. This can introduce additional delay to the VoIP traffic.

It is important to be aware that certain applications running over IP can set the frames with the "may fragment" bit to 1, which prevents fragmentation. As part of the overall assessment process, the network analysis on the LAN can determine if any applications have this bit setting.

Link speeds

Link speeds in a WAN environment are usually low compared to a LAN. When considering VoIP in a WAN environment, link speeds are an important consideration, as speeds under 1 Mbps result in the serialization delay of VoIP packets. This can impair deployment. When smaller VoIP packets travel over a network that typically has packet sizes up to 1500 bytes, these larger packets introduce variable delay (jitter) in the network. This impacts voice quality.

To address delay on a WAN, implement the following:

- protocol prioritization
- traffic shaping (for Frame Relay)
- DiffServ
- fragmentation and interleaving (larger packet sizes incur higher serialization delays and introduce jitter into the VoIP stream)

Other vendor devices also have several mechanisms available.

If link speed and packet size are considered, the serialization delay introduced can be predicted. See "Serialization delay" on page 130 for more information.

Recommendation

Nortel strongly recommends beginning with an MTU size of 232 bytes for links under 1 Mbps, adjusting upwards as needed.

Some applications do not perform well with an adjusted MTU, so caution must be used when utilizing MTU.

Link types

Identify and document the link types used in the network. A number of different link types are available in the network and each can have an impact on VoIP.

A typical campus network can have 100 Mbps of bandwidth going to the desk, with multi-gigabit riser links. Since bandwidth is plentiful, peak link utilization is the most important issue. If link utilization is averaged, it may not be accurate. A minimum of Layer 2 switching is required, with no shared media.

Point-to-point links (PPP)

PPP links are direct point-to-point links, and give the network operator maximum control over QoS. PPP links provide dedicated bandwidth and flexible termination points.

Frame Relay

Frame Relay (FR) networks provide more flexibility when the requirements include a full meshed topology. They have a lower overall cost, with respect to meshed designs.

Frame Relay networks are based on a shared-access model, where Data Link Connection Identifier (DLCI) numbers are used to define Permanent Virtual Circuits (PVCs) in the network.

QoS in a Frame Relay network is achieved by specifying a Committed Information Rate (CIR) and using separate PVC's. CIR is the level of data traffic (in bits) that the carrier agrees to handle, averaged over a period of time.

The CIR on the voice traffic PVC must be set for the total peak traffic, because any traffic that exceeds the CIR is marked Discard Eligible (DE) and can be dropped by the carrier. This is not an acceptable condition for VoIP traffic, as real-time data carrying packetized voice cannot be retransmitted.

It is important to understand the design of the carrier network, how much traffic is currently being transported, and if any type of Service Level Agreement (SLA), other than CIR, is offered.

The WAN-access platform in the network can help ensure that VoIP traffic does not exceed the CIR on the PVC. Protocol prioritization, traffic shaping and fragmentation can insure that the VoIP traffic is transmitted first and does not exceed the CIR on the PVC.

Asynchronous Transfer Mode (ATM)

ATM transport can provide a Constant Bit Rate (CBR) service, dedicating a channel with a fixed bandwidth based on the application's needs.

Using ATM as a transport for VoIP adds overhead associated with ATM. A G.711 CODEC with 20 ms voice payload, when the associated TCP, UDP, and RTP header information is added, can become a 200-byte frame.

Using ATM for transport requires the frame to be segmented to fit into multiple cells. This adds an additional 10–15% of overhead. The G.729 CODEC significantly reduces the frame size to 60 bytes, so CODEC selection is crucial for the WAN.

Virtual Private Network

A Virtual Private Network (VPN) is a network that uses the public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. Encryption and other security mechanisms are used to ensure that only authorized users can access the network and that the data cannot be intercepted.

Link utilization assessment

To support VoIP over WAN links, it is important to assess link utilization. There are several ways to gather statistical information on a WAN link. Tools such as an existing network management system should have the ability to poll routers through SNMP and collect the statistics over a period of time on utilization of a given WAN link.

Other methods of assessment include the use of imbedded Remote Monitoring (RMON) and external RMON probes installed for the purpose of gathering statistical information, including link utilization.

Over low-bandwidth connections, the amount of VoIP traffic should be limited to a percentage of the bandwidth of the connection. This is done to minimize the maximum queuing delay that the VoIP traffic experiences over low-bandwidth connections.

Assessing link utilization

WAN links are the highest repeating expenses in the network and they often cause capacity problems in the network. Unlike LAN bandwidth, which is virtually free and easily implemented, WAN links take time to finance, provision, and upgrade, especially inter-LATA (Local Access and Transport Area) and international links. For these reasons, it is important to determine the state of WAN links in the intranet before installing the network.

IMPORTANT!

The use of QoS mechanisms which prioritize voice over data traffic effectively increases the amount of bandwidth available to voice traffic.

To assess the link utilization, follow the steps in Procedure 1.

Procedure 1

Assessing link utilization

- 1 Obtain a current topology map and link utilization report of the intranet.
- 2 Visually inspect the topology map to reveal which WAN links are likely to deliver IP Line traffic. Alternately, use the Traceroute tool (see "Network performance measurement tools" on page 108).
- 3 Determine the current utilization of the WAN links. Note the reporting window that appears in the link utilization report. For example, use of the link use can be averaged over a week, a day, or an hour.
- 4 Obtain the busy period (peak hour) use of the link.
- 5 Since WAN links are full-duplex and data services exhibit asymmetric traffic behavior, obtain the utilization of the link representing traffic flowing in the heavier direction.

- 6 Assess how much spare capacity is available.

Enterprise intranets are subject to capacity planning policies that ensure that capacity usage remains below pre-determined level.

For example, a planning policy states that the use of a 56 Kbps link during the peak hour must not exceed 50%; for a T1 link, the threshold is higher, perhaps 80%. The carrying capacity of the 56 Kbps link would therefore be 28 Kbps, and for the T1, 1.2288 Mbps. In some organizations, the thresholds can be lower than that used in this example; in the event of link failures, there needs to be spare capacity for traffic to be rerouted.

- 7 Obtain the QoS parameters (in addition to the physical link capacity), especially the Committed Information Rate (CIR) for Frame Relay and Maximum Cell Rate (MCR) for ATM.

Some WAN links can be provisioned on top of Layer 2 services such as Frame Relay and ATM; the router-to-router link is actually a virtual circuit, which is subject not only to a physical capacity, but also to a "logical capacity" limit.

- 8 The difference between the current capacity, and its allowable limit, is the available VoIP capacity.

For example, a T1 link used at 48% during the peak hour, with a planning limit of 80%, has an available capacity of about 492 Kbps.

End of Procedure

Traffic flows in the network

Identify traffic flows in the network by using an existing Network Management System (NMS) or another passive tool, such as a packet sniffer. These tools identify protocol distribution in the network and traffic flow between devices. RMON probes and devices with embedded RMON capability can also help the network designer determine where traffic flows occur.

Assess traffic flows over a period of time (a week or longer depending on the complexity of the network). Observe the peak times of the day, the week, and the month to determine the highest utilization periods.

Once traffic flows are identified, determine bandwidth requirements using tools such as a VoIP bandwidth calculator. Ask your Nortel representative for

the VoIP bandwidth calculator spreadsheet. For more information, see “VoIP Bandwidth Demand Calculator” on page 117.

Available traffic tools

There are many tools available for assessing network traffic flows. Some of these include:

- Traceroute
- Call Detail Record
- Traffic study
- Network Diagnostic Utilities (refer to “Network Diagnostic Utilities” on page 229)

Traceroute

Traceroute uses the IP TTL (time-to-live) field to determine router hops to a specific IP address. A router must not forward an IP packet with a TTL field of 0 or 1. It must instead throw away the packet and return to the originating IP address an ICMP “time exceeded” message. Traceroute uses this mechanism by sending an IP datagram with a TTL of 1 to the specified destination host.

The first router to handle the datagram sends back a “time exceeded” message. This identifies the first router on the route. Then Traceroute sends out a datagram with a TTL of 2. This causes the second router on the route to return a “time exceeded” message and so on until all hops have been identified. The Traceroute IP datagram has a UDP Port number unlikely to be in use at the destination (usually > 30 000). This causes the destination to return a “port unreachable” ICMP packet, thereby identifying the destination host.

Traceroute can be used to measure roundtrip times to all hops along a route, thereby identifying bottlenecks in the network.

Call Detail Record

Obtain a Call Detail Record (CDR) to locate the VoIP traffic flows in the network. The CDR can help identify the network routes that VoIP will use.

The peak values for time of day, day of week, and day of month must be considered to ensure consistent voice quality.

For more information, refer to *Call Detail Recording: Description and Formats* (553-3001-350).

Traffic study

Traffic is a measurement of a specific resource's activity level. LD 02 has been reserved for scheduling and selecting the traffic study options.

A network traffic study provides information such as:

- the amount of call traffic on each choice in each route list
- the number of calls going out on expensive routes in each route list
- queuing activity (Off-Hook Queuing and Callback Queuing) and the length of time users queue, on average

For more information on traffic studies, refer to:

- *Traffic Measurement: Formats and Output* (553-3001-450)
- LD 02 in *Software Input/Output: Administration* (553-3001-311)

Service level agreements

As part of their service level agreement, the service provider should guarantee a certain amount of bandwidth.

Whether a home user on a cable or DSL connection, or a large network customer using Frame Relay, the service provide must guarantee bandwidth for VoIP.

Guaranteed bandwidth in Frame Relay, for example, is known as Committed Information Rate (CIR). The guaranteed bandwidth must be sufficient to accommodate all of the network traffic. Ensure that the CIR rate that was contracted is received when leasing a connection.

Exercise caution if service level agreements are not available.

Summary

It is crucial to fully understand the existing data network design before implementing a VoIP network. There are many considerations that are important when creating a new converged voice and data network. Network design tools are available to assist with this process.

QoS mechanisms

Contents

This section contains information on the following topics:

Introduction	48
Traffic mix	50
TCP traffic behavior	50
QoS problem locations	51
Campus networks	52
Wide Area Networks	53
The QoS process	53
Classification	54
Marking	55
Queuing	55
WAN QoS mechanisms	57
Bandwidth demand	58
Fragmentation and interleaving	59
Traffic Shaping	62
RTP header compression	64
PPP QoS	64
Frame Relay QoS	64
ATM QoS	65
Layer 2 (Ethernet) QoS	65
MAC address	66
IEEE 802.1Q	66
Port prioritization	69

Layer 3 QoS	72
IP address classification	72
DiffServ for VoIP	72
Trust configuration	74
Voice signaling and media DSCPs	75
Setting DSCP values	75
OTM and Element Manager QoS configuration	78
Layer 4 (TCP/IP) classification	80
Port number classification	81
Protocol ID classification	81
CS 1000 and Meridian 1 ports	81
Policy management	81
Optivity Policy Services	81
Bandwidth Management	82
VoIP bandwidth management zones	84
Interzone vs. Intrazone	87
Bandwidth Management is nodal	88
VPN1 and Zone numbers	88
Relationship between zones and subnets	90
Adaptive Bandwidth Management	90
CODEC selection	90
VoIP network voice engineering considerations	91

Introduction

This section describes the mechanisms required to design a QoS-managed VoIP network with satisfactory voice quality.

Today's corporate intranets evolved to support data services that found a "best effort" IP delivery mechanism sufficient. Standard intranets are designed to support a set of QoS objectives dictated by these data services.

An IP network must be properly engineered and provisioned to achieve high voice quality performance. The network administrator should implement QoS policies network-wide so voice packets receive consistent and proper treatment as they travel the network.

IP networks that treat all packets the same are called "best-effort networks". In such a network, traffic can experience different amounts of delay, jitter, and loss at any given time. This can produce the following problems:

- speech breakup
- speech clipping
- pops and clicks
- echo

A best-effort network does not guarantee bandwidth at any given time.

The best way to guarantee bandwidth for voice applications is to use QoS mechanisms in the intranet when the intranet is carrying mixed traffic types.

QoS mechanisms ensure bandwidth is 100% available at most times, maintaining consistent, acceptable levels of loss, delay, and jitter, even under heavy traffic loads.

QoS mechanisms are extremely important to ensure satisfactory voice quality. If QoS mechanisms are not used, there is no guarantee that the bandwidth required for voice traffic will be available. For example, a data file downloaded from the intranet could use most of the WAN bandwidth unless voice traffic has been configured to have higher priority. If the data file download could use most of the available bandwidth, this would cause voice packet loss, and therefore poor voice quality.

Recommendation

Nortel strongly recommends implementing suitable QoS mechanisms on any IP network carrying VoIP traffic.

This section describes QoS mechanisms that work in conjunction with the CS 1000 node. This section also discusses the intranet-wide consequences if the mechanisms are implemented.

Apply QoS mechanisms to the following VoIP media and signaling paths:

- TLAN connections

- VoIP traffic between IP Phones
- VoIP traffic between IP Phones and Voice Gateway Media Cards on the TLAN subnet

Traffic mix

Before implementing QoS mechanisms in the network, assess the traffic mix of the network. QoS mechanisms depend on the process and ability to distinguish traffic by class to provide differentiated services.

If an intranet is designed to deliver only VoIP traffic, and all traffic flows are of equal priority, then there is no need to consider QoS mechanisms. This network would only have one class of traffic.

In most corporate environments, the intranet primarily supports data services. When planning to offer voice services over the intranet, assess the following:

- Are there existing QoS mechanisms? What are they? VoIP traffic should take advantage of established mechanisms if possible.
- What is the traffic mix? If the volume of VoIP traffic is small compared to data traffic on the intranet, then IP QoS mechanisms will be sufficient. If VoIP traffic is significant, data services might be impacted when those mechanisms are biased toward VoIP traffic.

TCP traffic behavior

The majority of corporate intranet traffic is TCP-based. Unlike UDP which has no flow control, TCP uses a sliding window flow control mechanism. Under this scheme, TCP increases its window size, increasing throughput, until congestion occurs. Congestion is detected by packet losses, and when that happens throughput quickly throttles down, and the whole cycle repeats. When multiple TCP sessions flow over few bottleneck links in the intranet, the flow control algorithm can cause TCP sessions in the network to throttle at the same time, resulting in a periodic and synchronized surge and ebb in traffic flows. WAN links appear to be congested at one period of time and then are followed by a period of under-utilization. Two consequences are:

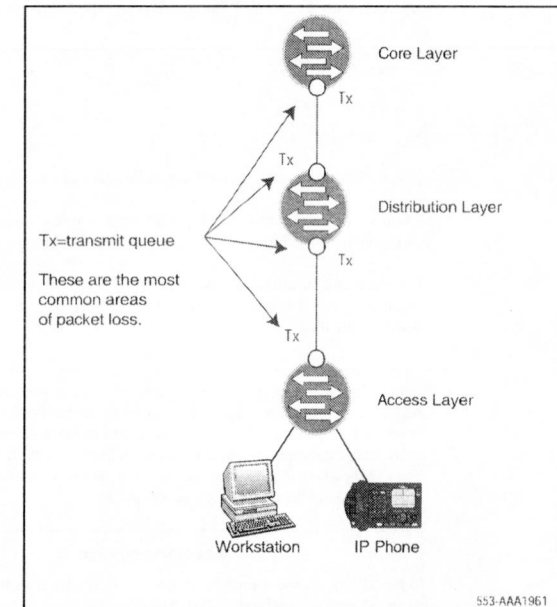
- WAN link inefficiency.
- VoIP traffic streams are unfairly affected.

The solution to this problem is Weighted Random Early Detection queueing (WRED) as described on page 55.

QoS problem locations

Figure 6 on page 52 identifies typical network congestion areas. Voice traffic competes for limited bandwidth on the uplinks. These uplinks are shown in Figure 6 on page 52. Congestion at these points causes the majority of all packet loss, delay, and jitter. QoS mechanisms can alleviate this congestion by using multiple queues with different priorities.

Figure 6
Potential uplink problem areas



Campus networks

In most cases, campus Ethernet networks require less sophisticated QoS mechanisms than low-bandwidth WAN connections, because the available bandwidth is much greater. This results in significantly lower queuing and network delay. However, network congestion on an Ethernet network (even for short periods of time) and bursty TCP-based Internet traffic can cause significant voice quality problems if QoS is not applied.

QoS mechanisms, such as 802.1Q, VLANs, and Layer 2 Port prioritization (802.1p), can be used for VoIP traffic over Ethernet networks. If the Layer 2 (Ethernet) switches also support Layer 3 (IP) capabilities, then QoS mechanisms such as DiffServ and IP Address prioritization can also be used. For example, the Business Policy Switch (BPS) is a Layer 2 switch that can recognize, filter, monitor, and re-mark 802.1p and DiffServ markings, based on implemented policy.

Wide Area Networks

A Wide Area Network (WAN) is a geographically-dispersed telecommunications network. For example, a WAN can extend across many cities or countries.

WANs require more sophisticated QoS mechanisms such as:

- fragmentation
- interleaving
- ATM
- Frame Relay

For more information, refer to "WAN QoS mechanisms" on page 57.

The QoS process

Packet handling on a QoS-enabled network consists of three stages:

- 1 Classification
- 2 Marking
- 3 Queueing, also known as Forwarding

To implement QoS on an IP network, all packets entering the IP network must be classified and marked. The packets are then placed into transmission queues of a certain priority.

Packets in high priority queues are transmitted before packets in best-effort lower priority queues. This means that VoIP packets no longer have to compete with best-effort data packets for IP network resources. Typical QoS implementations protect call quality by minimizing loss, delay, and jitter. Bandwidth cannot be assured without the use of some type of reservation protocol, such as Resource Reservation Protocol (RSVP).

Classification

Software on the following hardware elements can classify and mark VoIP packets:

- Signaling Server - classifies its packets as signaling packets
- Voice Gateway Media Card - classifies its packets as voice or signaling packets
- IP Phones - classify their packets as voice or signaling packets

Note: To classify Signaling Server and Voice Gateway Media Card packets at Layer 2 (802.1p) and/or Layer 3 (DiffServ), implement QoS mechanisms on the Signaling Server and Voice Gateway Media Card and the Layer 2 switch ports to which they are attached. IP Phones with firmware 1.31 (or later) can classify voice and signaling packets at Layer 2 (802.1p) and/or Layer 3 (DiffServ).

Classification can be implemented on Layer 2 or Layer 3 switches. Refer to the switch's documentation for information on configuring classification.

Policy management also provides other methods of classifying and marking packets, based on identifiers such as the originating IP address of the packet. For more information on Policy Management, see "Policy management" on page 81.

Packets can also be pre-marked with default 802.1p and DiffServ CodePoint (DSCP) values. Configure the Layer 2/Layer 3/Policy switches to trust that these packets are marked correctly.

Marking

When powered-up, Nortel IP Phones contact the Terminal Proxy Server (TPS) that controls them. The TPS then instructs the IP Phones to mark all packets with a default, yet configurable (through CS 1000 Manager) DSCP and/or 802.1Q/802.1p tag. The tag is also configurable using CS 1000 Element Manager.

The control packets are marked for each of the following:

- Signaling Server
- Voice Gateway Media Cards
- Media Gateway 1000T (MG 1000T)
- Network Routing Service

Queuing

Queuing delay is a major contributor to delay, especially on highly-utilized and low-bandwidth WAN links (see "Queuing delay" on page 131). Routers that are QoS-aware and that support priority queuing can help reduce the queuing delay of voice packets when these packets are treated with preference over other packets.

Weighted Random Early Detection (WRED)

The global synchronization situation described in "TCP traffic behavior" on page 50 can be countered using a buffer management scheme that discards packets randomly as the queue starts to exceed a threshold. Weighted Random Early Detection (WRED), an implementation of this strategy, also inspects the DiffServ bits in the IP header when considering which packets to drop during buffer build up. In an intranet environment where TCP traffic dominates real-time traffic, WRED can be used to maximize the dropping of packets from long-lived TCP sessions and minimize the dropping of voice packets. Check the configuration guidelines with the router vendor for performance ramifications when enabling WRED. If global synchronization is to be countered effectively, implement WRED at core and edge routers.

Packet prioritization and schedulers for VoIP

All VoIP packets must be given a priority higher than the priority of non-voice packets to minimize delay, jitter (delay variation), and packet loss which adversely affect voice quality.

Note: All voice packets must be placed in the highest priority queue using a strict-priority scheduler, or a scheduler that can be configured to behave as a strict-priority scheduler. Some switches only permit network-controlled traffic in the highest priority queue, leaving the second highest priority queue for the remaining user traffic.

Recommendation

Nortel strongly recommends that voice traffic be placed in a queue separate from other traffic types. However, if there are few queues available in the Layer 2 or Layer 3 switch, then voice traffic can be combined with other high-priority network-controlled traffic. Because the queuing delay is small for Ethernet network interfaces, this should have very little impact on voice quality.

Most Layer 2 switches use a strict-priority scheduler. A strict-priority scheduler schedules all packets in a higher-priority queue before servicing any packets in a lower priority queue.

All VoIP packets must be queued in a router or switch using a strict priority scheduler. This ensures that VoIP packets receive priority treatment over all other packets. Because a strict priority scheduler can "starve" the servicing of all other traffic queues, a threshold must be set to limit the maximum amount of bandwidth that the VoIP traffic can consume. This threshold is also called "rate limiting".

Recommendation

Nortel strongly recommends that a strict priority scheduler be used for VoIP.

The Business Policy Switch (BPS) places the voice packets in the highest priority queue using a strict-priority scheduler in its 4-queue system, when QoS is enabled on an interface.

Note: Other vendors often refer to "priority queueing" when describing their techniques for strict-priority scheduling.

Some Layer 3 switches and routers support priority and weighted schedulers. Voice packets must be placed in a queue that uses a strict-priority scheduler, or in a queue that uses a weighted scheduler configured to behave like a strict-priority scheduler.

The Passport 8600 uses a weighted scheduler, with its highest priority user queue configured by default to behave like a strict-priority scheduler. The queue is configured with all Packet Transmit Opportunities (PTOs) enabled. This is equivalent to a weight of 100% (highest priority). Voice packets with DSCPs marked with 'EF' (Expedited forwarding) and 'CS5' (Class Selector 5) are placed in this queue by default when QoS is enabled on an interface.

Nortel does not recommend other weighted schedulers, such as Weighted Round Robin (WRR) or Weighted Fair Queuing (WFQ). If the router or switch does not support a priority scheduler and only supports a weighted scheduler, then the queue weight for VoIP traffic should be configured to 100%. If a 100% weight cannot be configured due to some product limitation, then consider replacing the product, because it can cause unpredictable voice quality.

WAN QoS mechanisms

There are many things to consider when using routers with low-bandwidth WANs and low bandwidth access network connections such as T1, xDSL, or Packet Cable.

This section specifically discusses WAN connections, but the techniques and recommendations described also apply to low-bandwidth access network connections.

Bandwidth demand

One of the main attractions of VoIP is the ability to use an existing WAN data network to save on inter-office toll calls. However, offices often connect over low-bandwidth WAN connections, so special considerations must be made when adding VoIP over a bandwidth-limited connection.

When VoIP calls are active, routers configured with QoS (which prioritizes voice traffic over data traffic) reduce the data traffic throughput by the amount of bandwidth being used for the VoIP call. This reduces the data traffic throughput to a possibly unacceptable level. Adding VoIP to the existing WAN data network might require an increase in the WAN bandwidth.

VoIP bandwidth is dependent on the following:

- type of CODEC used
- Voice Activity Detection (VAD), if used; also known as Silence Suppression
- packetization rate (voice sample size)
- IP/UDP/RTP encapsulations
- RTP Header Compression, if used
- Layer 2 (link layer) protocol overhead for the specific link the voice traffic is traversing. Depending on the link protocol used and the options invoked, the link protocol adds the following to each VoIP packet:
 - 5 to 6 octets (FR)
 - 7 to 8 octets (PPP)
 - 18/22-26/30-38/42 octets (802.3 LAN – with or without 802.1Q/802.1p 8-octet preamble and 12-octet interframe gap)

The extra octets create an additional overhead of 2 kbps (5-octet FR) to 16.8 kbps (42-octet 802.3 LAN) for each VoIP call.

Note: ATM has its own overhead requirements. Due to the fixed cell size of 53 octets, the additional overhead varies widely, depending on the CODEC and packetization rate used.

Bandwidth example

A company has two sites connected by a leased-line WAN connection (PPP) operating at 128 kbps. Due to the potential use of 20% of link capacity for "zero-bit stuffing", a safe assumption for link capacity is 102 kbps. For design purposes, assume a maximum utilization of 70% (in this example, 90 kbps).

This bandwidth has been sufficient for the current data requirements. The company believes that it only needs 70-80 kbps most of the time, with occasional traffic peaks up to the full capacity. The company wants to support up to 4 simultaneous voice calls over the IP WAN network between the sites.

If all 4 calls were simultaneously active, this would require 108.8 kbps (using a G.729 CODEC, 20 ms voice sample, and PPP overhead/frame) of the available 90 kbps of the 128 kbps link.

This requirement exceeds the carrying capacity of the link and completely starves that data traffic. The solution is to upgrade the WAN connection bandwidth. A 256 kbps link is the minimum speed to provide 109 kbps for four G.729 VoIP calls, 80 kbps for data, and 20% availability for zero-bit stuffing.

Fragmentation and interleaving

To minimize voice delay and jitter in mixed voice/data IP networks, fragment large packets before they traverse limited-bandwidth (<1 Mbps) connections. There are several different protocols that can be used to fragment packets.

For Frame Relay connections, the FRF.12 standard can be used for fragmenting packets. ATM provides fragmentation since all packets are fragmented into 53-byte ATM cells. Both of these fragmentation techniques are acceptable.

Two types of fragmentation are more universal and not limited to a specific link-layer technology, such as ATM or Frame Relay. These methods are PPP fragmentation and IP fragmentation.

Refer to the router's documentation for information on configuring PPP and IP fragmentation.

Layer 2 fragmentation (ATM, FRF.12, PPP) is preferred over Layer 3 fragmentation, as Layer 2 fragmentation universally affects all higher layer protocols. Layer 3 fragmentation is less desirable for two reasons:

- 1 Layer 3 fragmentation applies only to the specific protocol being used. For example, Internet Protocol's Maximum Transmission Unit (MTU, in bytes) affects only IP traffic. It has no effect on IPX, AppleTalk, or other protocols.
- 2 Some applications do not function because they set the "Do not Fragment" bit. This prevents the application's packets from being transmitted.

PPP fragmentation and interleaving

Many routers support PPP fragmentation. PPP fragmentation splits large packets into multiple smaller packets and encapsulates them into PPP frames before they are queued and transmitted. PPP fragmentation enables higher-priority VoIP packets to be transmitted ahead of the lower-priority data packet fragments that have already been queued. The voice packets and data fragments are interleaved so the maximum delay a voice packet will experience is one fragment time (ideally <=10 ms), rather than one large packet time.

For example, a small voice packet enters a router, followed by a large data packet, which is followed by a second voice packet. The first voice packet is transmitted as the first frame on the link. Next, the first data fragment is transmitted, followed by the second voice packet, then the second data fragment. If no more packets enter the router for a time, then the remaining data fragments will continue to be transmitted until the entire data packet has been sent.

Interleaving is a result of voice packets having a higher priority than data packets. A data fragment can be transmitted first; however, when a high-priority voice packet arrives, the voice packet will be sent before the rest of the data packet.

IP fragmentation

All routers support IP fragmentation. IP fragmentation configures all IP packets to a size determined by the MTU (Maximum Transmission Unit). Most routers use a default maximum packet size of 1500 bytes (the largest

packet allowed on Ethernet LANs), which can take a considerable amount of time to transmit over a low-bandwidth connection.

**CAUTION**

When determining the fragment size for a packet, ensure that the fragment size is not smaller than the voice packet. Fragment only the larger data packets, not the voice packets.

For example, over a 64 kbps link, a 1500-byte data packet takes 188 ms to transmit. If the WAN connection is Frame Relay (FR), this same queuing delay is added again when the packet is queued at the far-end FR switch on the other side of the connection. To achieve high voice quality, the desirable end-to-end delay for a voice packet is less than 150 ms. In this example, the data packet uses up almost the entire delay budget for the voice traffic before the first voice packet is ever transmitted. Jitter of 188 ms is created, which greatly exceeds the normal jitter buffer settings of 2 to 3 voice sample sizes (40 – 90 ms). This results in at least one packet, and usually many packets, arriving too late to be used.

Over bandwidth-limited connections (<1 Mbps), if Layer 2 (ATM, FRF.12, or PPP) fragmentation is not used, the router must be configured to transmit smaller packets by adjusting the MTU size for the IP packets. Ideally, the MTU size is adjusted to achieve an optimum delay of 10 ms or less over the different connection speeds. Therefore, a higher bandwidth connection will have a larger MTU size than a lower bandwidth connection.

Note: When IP fragmentation is used, the packets remain fragmented from source to destination. This can result in reduced data performance since the larger data packets are fragmented into multiple, smaller fragments that use more bandwidth.

Table 3 on page 62 provides the recommended maximum MTU sizes for different connection speeds when using IP fragmentation. These choices result in a maximum delay of 8 ms.

Note: These values also apply to Layer 2 fragmentation techniques.

Table 3

Recommended MTU sizes for various connection speeds

	Connection Rate (in kbps)				
	56	64	128	256	512
Maximum MTU size (in bytes)	56	64	128	256	512

Recommendation

Nortel strongly recommends PPP as the preferred method for packet fragmentation. Use IP fragmentation only if the router does not support a Layer 2 fragmentation protocol, such as PPP or FRF.12.

Packet reordering

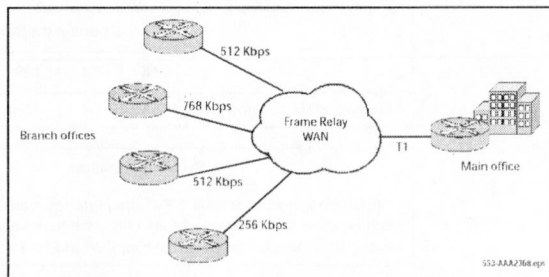
In some cases, there can be multiple paths for a VoIP packet to take when traveling from source to destination. If all VoIP packets do not take the same path, packets can arrive out-of-order. This can cause voice quality issues, even though packet reordering often has little or no adverse affect on data traffic quality, due to the design of the data protocols.

For example, if two locations are connected using two Frame Relay Permanent Virtual Circuits (PVCs), it is necessary to ensure that all voice traffic for a specific call travels on the same PVC. The routers can be configured to direct voice packets from the same source/destination IP address to traverse the same PVC. Another approach is to configure the router to send all voice traffic over only one PVC.

Traffic Shaping

In a Frame Relay environment, a typical design could have many low-speed links, terminating at Media Gateway 1000B (MG 1000B) locations with a single high-speed link into a hub location. See Figure 7 on page 63.

Figure 7
Traffic shaping



In this example, the MG 1000B sites with a low speed link can be overrun by traffic from the central site that has a larger bandwidth connection. Or the main office site could be overrun with traffic from all of the MG 1000B sites. Without traffic shaping, the network can randomly drop packets. The resulting packet loss is detrimental to voice quality.

Traffic shaping prevents this from happening. Through the use of traffic shaping, it is possible to determine which packets are dropped due to congestion and which packets receive priority.

Traffic shaping works by queuing excess traffic to lower the amount of bandwidth across a Frame Relay WAN to limit traffic to a predetermined level. This is known as the Committed Information Rate (CIR). CIR is negotiated with the service provider.

If data is offered too fast and the Committed Burst (Bc) rate plus the Excess Burst (Be) rate exceeds the CIR over a certain Time Interval (Tc), the Frame Relay network can mark any packets as Discard Eligible. This cannot be tolerated when running real-time applications such as voice.

When running traditional data applications over Frame Relay, the network allows bursting over a certain Time Interval (Tc). If the data burst exceeds the contract during that time interval, the Frame Relay network starts sending

Layer 2 (L2) feedback in the form of Forward Explicit Congestion Notifications (FECN) and Backward Explicit Congestion Notifications (BECN). This L2 feedback informs the Data Terminal Equipment (DTE) devices (routers) that congestion is occurring in the upstream or downstream direction. Upon receiving this feedback, the DTE should throttle back to the Committed Burst (Bc) or a fraction of the Bc. It is also possible for the DTE to completely shutdown until the feedback indication abates for a period of time.

While this is considered a benefit for data applications, the resulting packet loss is detrimental to quality.

RTP header compression

IP Real-time Transport Protocol (RTP) header compression can be used to compress 40-byte (IP, UDP, RTP) VoIP packet headers down to a size of 2 to 4 bytes.

This results in significant bandwidth savings across low-bandwidth WAN links. It is important to note current WAN platform CPU levels before implementing RTP header compression, because it is CPU intensive.

PPP QoS

It is important that QoS mechanisms are used over low-bandwidth links that carry both voice and data traffic.

Implementing QoS mechanisms over a PPP WAN link may involve the use of the following:

- priority queuing (possibly mapped from the Diffserv CodePoint (DSCP))
- RTP header compression
- fragmentation and interleaving

Frame Relay QoS

Nortel recommends separate Permanent Virtual Circuits (PVCs) for voice and data whenever possible. Ensure voice PVCs strictly conform to the CIR.

Do not allow bursting or shaping. It can be beneficial to use partially meshed PVCs, depending on traffic patterns.

If voice and data traffic share the same PVC, it can be necessary to use priority queuing along with traffic shaping to ensure that voice packets are not discarded or queued for a long period time. On low bandwidth links (<1 Mbps), fragmentation and interleaving (FRF.12) may have to be used.

ATM QoS

Two methods of ensuring VoIP QoS on ATM links are available:

- separate voice and data PVCs
- priority queuing on a shared voice and data PVC

Nortel recommends separate voice and data PVCs. The available bandwidth for a particular ATM PVC is usually guaranteed by a service provider. If traffic through the PVC is restricted to VoIP traffic only, then no other QoS mechanisms in the ATM network must be used. Voice traffic can be mapped into the voice-only PVC according to source IP address or Diffserv CodePoint. VoIP bandwidth management on the Call Server can then be used to ensure that the VoIP traffic volume does not exceed the amount of bandwidth available in the voice-only PVC.

If a shared voice and data PVC is used, then priority queuing must be configured across the ATM network to guarantee that voice traffic has priority over data traffic.

Layer 2 (Ethernet) QoS

At Layer 2, VoIP packets can be classified by the following fields in the Ethernet header:

- source/destination MAC address
- 802.1Q
 - VLAN ID
 - 802.1p user priority bits

MAC address

All MAC addresses are unique and should not be changed.

Packets can be classified by the MAC address. Packets from a Nortel IP Phone can be recognized because each Nortel IP Phone has a unique set of MAC addresses. When the Layer 2 switch recognizes the IP Phone packet's MAC address, it marks the packets with the appropriate 802.1p value. Then the Layer 2 switch places the packets in the correct switch queue. The correct queue is determined by the QoS policy implemented by the network administrator.

IEEE 802.1Q

The IEEE 802.1Q standard extends the Ethernet frame format by adding four bytes to the Ethernet packet header. See Figure 8.

The 802.1Q extensions contain two important fields – the 802.1p field and the VLAN ID field. Table 4 on page 67 lists the 802.1Q field names and their definitions.

Figure 8
Ethernet 802.1Q extensions

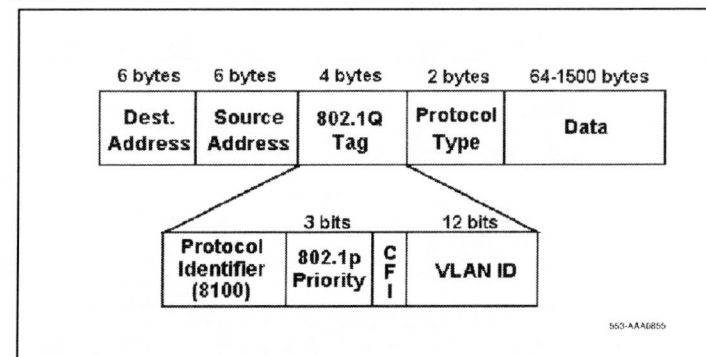


Table 4
IEEE 802.1Q field definitions

802.1Q field	Description
Tag protocol identifier	Always set to 8100h for Ethernet frames (802.3 tag format)
3-bit priority field (802.1p)	Value from 0-7 representing user priority levels (7 is the highest)
Canonical field	Always set to 0 (zero)
12-bit 802.1Q VLAN ID	VLAN identification number

VLAN ID

A VLAN logically groups network devices into a single broadcast domain. Each VLAN has its own IP subnet. This ensures that devices on separate VLANs cannot communicate with each other unless their traffic is routed. The routing enables traffic separation and isolation by creating separate broadcast domains.

VLANs provide a popular method of supporting QoS, using a Layer 2 (Ethernet) switching structure.

Note: The routers must be compatible. Routers must support VLANs on their physical ports.

VLANs have obvious advantages when applied to voice traffic on an IP network. VLANs enable packets with similar QoS requirements to be grouped together to receive the same QoS treatment.

Note: When routing into a specific VLAN, configure the router interface to tag the incoming Layer 2 Ethernet frames with the correct VLAN ID and priority.

VLANs provide a useful way to separate and prioritize the IP telephony packets for Layer 2 switches. A telephony VLAN can be created so that all IP telephony devices are members. This enables the Layer 2 switch to prioritize all telephony traffic so that it all receives consistent QoS treatment.

Note: A VLAN can only provide QoS on Layer 2 switches that support the 802.1Q (VLAN) standard. Once the packets leave the Layer 2 switch, and encounter routers or WAN switches, DiffServ should be used to provide end-to-end QoS. Nortel IP Phones also mark the DSCP, so when voice packets encounter routers, the routers can be configured to prioritize the packets based on their DSCP value.

IP Phones 200x support IEEE 802.1Q using firmware version 1.39 or later. The default Ethernet Class of Service (CoS) is 0; this is the same as the 802.1Q priority bits.

The IP Phones 200x firmware tags the ethernet frames with both the telephone's VLAN ID and the 802.1p priority specified in Element Manager. The recommended 802.1p priority is 6.

The Nortel IP Softphone 2050 client support of IEEE 802.1Q priority depends on the underlying operating system and hardware.

802.1p user priority bits

The 802.1p field has three bits to provide eight Classes of Service (CoS). 802.1p-capable L2/L3 switches use these Classes of Service to prioritize packets, and then place them in different queues. This provides service differentiation.

802.1p configuration

Use Procedure 4 to configure the 802.1p priority bits in Element Manager.

Procedure 2 Configuring 802.1p priority bits in Element Manager

See *Element Manager: System Administration* (553-3001-332) for more information on Element Manager.

- 1 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the Element Manager navigator.
- 2 In the **Node Configuration** window, click **Edit** next to the node to be configured.

The Edit window opens, as shown in Figure 9 on page 69.

Figure 9
Priority bit configuration in Element Manager

- 3 Click **QoS**.
- 4 Select **Enable 802.1Q support**.
- 5 Enter the IP Phone priority in the **802.1Q Bits value (802.1p)** text box.

End of Procedure

Port prioritization

A Layer 2 switch port can be configured to prioritize all packets entering it. This could be done in cases where IP Phones connect to a Layer 2 switch port that is not shared with other devices.

3-port switch port prioritization

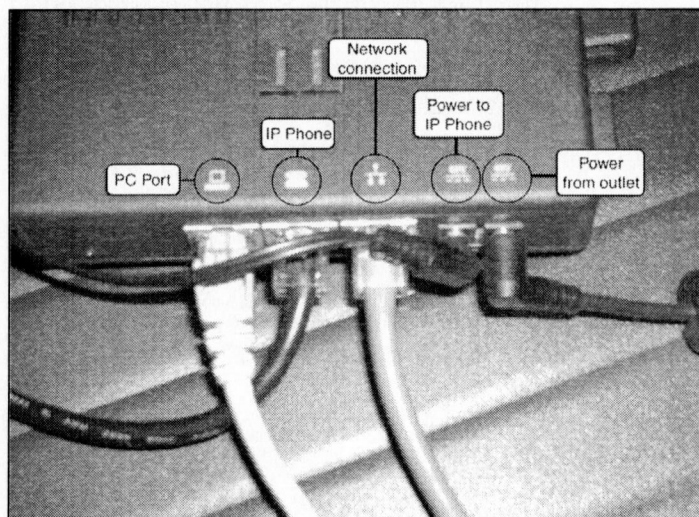
IP Phones have an optional external 3-port Layer 2 switch module that is inserted into the bottom of the phone. See Figure 10 on page 71.

The IP phones have a built-in 3-port switch. The internal port is used by the IP phone. The two external ports provide connection to the network and another device (such as a PC).

The 3-port Layer 2 switch enables a PC and an IP Phone to share a single Ethernet connection. All packets entering the port connected to the IP Phone are given a higher priority than packets entering the port connected to the PC. This ensures that all voice packets are sent ahead of any data packets. This has little effect on the data packets because the IP Phone packets are small and use little bandwidth.

Note: When using the optional external 3-port switch module, the IP Phone must be plugged into the correct port for the voice packets to receive proper treatment. See Figure 10 on page 71.

Figure 10
3-port switch



This approach has limitations. For example, if a network user unintentionally (or intentionally) connects a PC to the IP Phone Ethernet port, the user can unfavorably take advantage of network resources. This situation can be prevented by ensuring that all packets entering the port are also prioritized through MAC or VLAN ID classification to determine that they are from an IP Phone.

Recommendation

Nortel strongly recommends that, for stationary IP telephony devices such as VoIP gateways, use port prioritization on the Ethernet switch port that connects to the device.

Layer 3 QoS

DiffServ is the recommended Layer 3 QoS mechanism. Newer Layer 3 IP devices (routers and Layer 3 switches) can classify IP Phone packets by using the following fields in the IP packet header:

- source/destination IP address
- DiffServ CodePoint (DSCP)
(the 6 Most Significant Bits (MSB) in the 8-bit DiffServ field)

IMPORTANT!

The values entered in these two fields must be coordinated across the entire IP data network. Do not change them arbitrarily.

IP address classification

A Nortel IP Phone obtains its IP address in one of two ways:

- DHCP is used to automatically obtain the IP address.
- the IP address is permanently assigned through the keypad.

To make it easier to prioritize packets by IP addresses, a pool of IP addresses can be set aside exclusively for IP Phones. The Layer 3 switch/router can then prioritize the packets based on this range of IP addresses. It marks the voice packets from those designated IP addresses with the recommended DSCP.

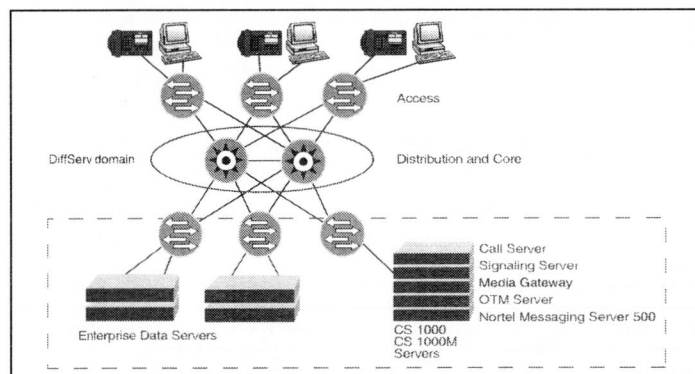
This method does not differentiate between voice media and signaling packets. Only a single DSCP is used for both. However, if additional filters are applied to sort the different packet types, the voice media and signaling packets can be marked with different DSCPs.

DiffServ for VoIP

DiffServ-based QoS at Layer 3 provides end-to-end QoS. By using DSCP, DiffServ enables service assignment to network traffic on a per-hop basis.

Figure 11 on page 73 shows the architecture of DiffServ-based QoS.

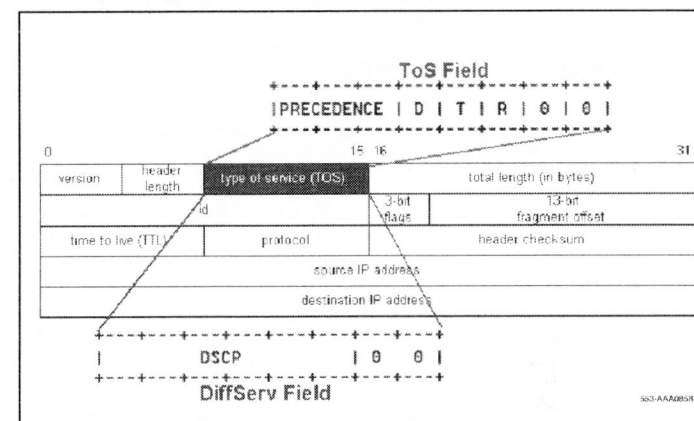
Figure 11
DiffServ-based QoS architecture



The DiffServ CodePoint (DSCP) is a 6-bit value contained in the second byte of the IPv4 header. See Figure 12 on page 74. The DSCP determines the DiffServ Per Hop Behavior (PHB) treatment that the router/Layer 3 switch provides to the IP packets.

The DSCP is contained in the 8-bit DiffServ Field (DS Field), formerly known as the Type of Service (ToS) Field. Some routers use the older ToS terminology instead of the newer DiffServ terminology. However, in either case, the six most significant bits in this field are the DSCP value. See Figure 12 on page 74.

Figure 12
IPv4 header showing DSCP location



Note: The 8-bit value, rather than the 6-bit value, is seen if using a network analyzer to look at the DiffServ byte.

Trust configuration

DiffServ edge routers and switch interfaces can be configured to trust or distrust any previously-marked DSCP or 802.1p-tagged packet. Voice packets entering 'untrusted' interfaces are re-marked to a DSCP/802.1p value of 0 (best effort), unless filters are set up to classify the packets and mark them with the DSCP or 802.1p value specified by the network administrator. If the router and switch interfaces are configured as 'trusted' interfaces, then the packets are not re-marked and the pre-marked voice packets are prioritized based on their DSCP and 802.1p values.

A router can use the DSCP to queue pre-marked IP Phone packets if they have arrived from a trusted source.

For example, a Layer 3 switch can have Ethernet ports assigned just to IP Phones. These ports can be configured to trust that the IP Phones have marked the packets correctly.

Voice signaling and media DSCPs

Over a high bandwidth, low latency Ethernet LAN connection, voice media packets and signaling packets can be placed in the same queue in the Layer 2 or Layer 3 switch. In this case, it is not necessary to differentiate between voice media packets and voice signaling packets.

However, when the voice packets use a low-bandwidth (less than 1 Mbps) connection, considerable queuing delay can occur. This queuing delay, when coupled with the arrival of different-sized voice packets (signaling and media), creates an unacceptable amount of voice jitter, which in turn results in poor voice quality.

To minimize voice jitter over low bandwidth connections, the voice media packets and voice signaling packets must be separated into different queues. By marking the voice media packets and voice signaling packets with a different DSCP, the packets can be classified and separated into different queues by the router connected to the low-bandwidth connection.

Note: It is important to categorize signaling packets so they are not discarded by the network. The IP Phone contains a watchdog timer that resets the IP Phone if signaling packets are not seen within a certain amount of time. Lost signaling packets can also cause the IP Phones to reset.

Setting DSCP values

If a best-effort network is currently in place, and VoIP is being added, the simplest approach is to create the network QoS with only three priority levels:

- 1 VoIP voice media traffic
- 2 VoIP signaling traffic
- 3 best-effort IP data traffic

Routers connected to low-bandwidth interfaces must separate voice media packets and voice signaling packets. This is necessary to minimize jitter that was introduced by the signaling packets to the voice media packets. This jitter occurs if the packets are placed in the same queue instead of separate queues.

IP packets are prioritized based on the DSCP in the distribution layer, core layer and WAN.

DiffServ is supported on the Signaling Server, Voice Gateway Media Cards, and the IP Phones.

Table 5 shows the recommended DiffServ traffic classes for various applications.

Table 5
Recommended DiffServ classes

Traffic type	DiffServ class	DSCP (binary)	DSCP (decimal)
Voice media	Expedited Forwarding	101110	46
Voice signaling	Class Selector 5	101000	40
Data traffic	default	000000	0

Note: If using Sniffer, the values in a sniffer capture are 8-bit values. The EF DSCP can appear as 184 decimal. The CS5 DSCP can appear as 160 decimal.

The Nortel standard DSCP for signaling is decimal 40.

The Nortel standard DSCP for voice is decimal 46, based on six bits of an 8-bit field. Two bits are unused.

The DSCP is configured in Element Manager.

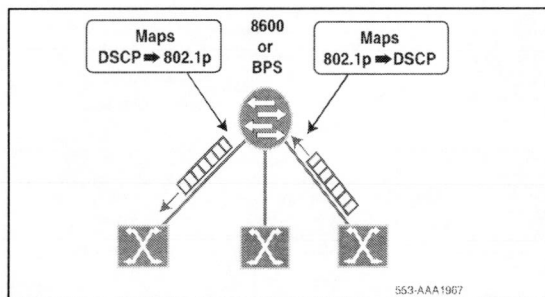
Mapping DSCP to 802.1Q

Some switches such as the Passport 8600 and Business Policy Switch can map the DSCP to and from an 802.1p tag. See Figure 13 on page 77.

This extends the IP QoS to Layer 2 QoS for the downstream Layer 2 switches that are not IP-aware. The Passport 8600 has a mapping table for DSCP to 802.1p. The Passport 8600 can map packets marked with "EF" and "CS5" DSCPs to 802.1p user priority '110'. The downstream Layer 2 switch should be configured to place this 802.1p tag of '110' into its highest priority queue.

If a network administrator has configured a different 802.1p tag for the IP Phone's packets, then packets tagged with this value should be placed in the highest priority queue of the Layer 2 switch. The network administrator must also ensure consistency in mapping the "EF" and "CS5" marked packets to this 802.1p tag.

Figure 13
Mapping DSCP to 802.1p



Example

Using Optivity Telephony Manager (OTM), a network administrator can configure the IP Phone 2004 controlled by a Voice Gateway Media Card to mark the voice media packets with the "EF" DSCP, and the voice signaling packets with the "CS5" DSCP.

The Passport 8600 routing switch trusts the premarked packets entering ports configured as "core ports". The Passport 8600 places these packets into the highest priority queue by default. The scheduler for this queue is

preconfigured with a Packet Transmit Opportunity (PTO) or queue weight of 100%.

This configuration provides the necessary behavior required for IP Phone packets to achieve the required QoS.

OTM and Element Manager QoS configuration

QoS configuration is done using OTM or Element Manager.

- Meridian 1 systems equipped with IP Trunk and IP Line must use OTM.
- CS 1000 systems must use Element Manager.

Adhering to Nortel standards, the DSCP bits for VoIP control packets are set to "CS5", decimal value of 40. The voice packets are set to the Expedited Forwarding decimal value of 46. By default, the Passport 8600 and BPS place the voice and control packets into the same queue.

For slower links (<1 Mbps), the control and voice packets marked with different DSCP values should be separated into different queues; otherwise, the voice packets experience significant queuing delays. Figure 14 on page 79 shows DSCP configuration using OTM.

Figure 14
Voice Gateway Media Card DiffServ CodePoint (DSCP) configuration through OTM

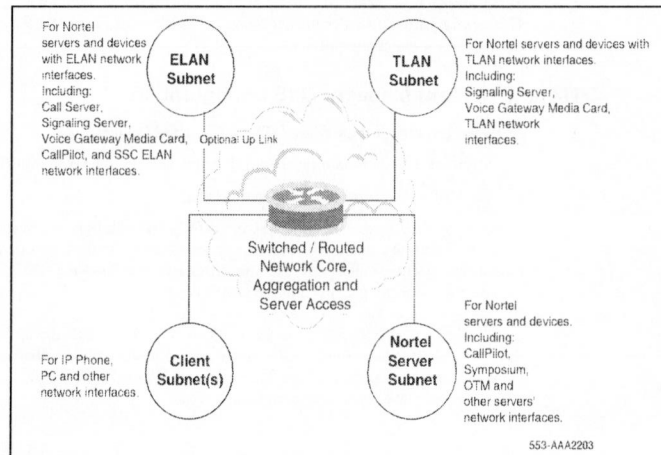


Figure 15 shows DCSP configuration using Element Manager.

Figure 15
Voice Gateway Media Card DSCP configuration through Element Manager

Layer 4 (TCP/IP) classification

All Layer 4 IP devices can classify IP Phone packets by using the following fields in the packet header:

- source/destination TCP/UDP port number
- protocol ID

Port number classification

UDP port numbers used by IP Phone RTP packets are dynamically assigned. This makes it difficult to classify packets by port number. However, if a specific range of port numbers is assigned to IP Phones, then the router recognizes that the packet has come from a port number assigned to IP Phones, and prioritizes the packet as a voice packet.

There is a disadvantage to using this method of prioritization. Another application can use the same port number range, causing its packets to be mistaken for voice packets and allowing packets to be assigned an incorrect QoS behavior and prioritization.

Protocol ID classification

The Real-time Transport Protocol (RTP) is used by many multimedia applications such as real-time fax and video, as well as voice. Prioritizing packets according to the protocol used, therefore, cannot be used to accurately prioritize the voice packets.

CS 1000 and Meridian 1 ports

See Appendix B: "Port number tables" on page 257 for more information.

Policy management

Prioritization of traffic can also be implemented through policy management. Nortel supports this option through Optivity Policy Services software.

Optivity Policy Services

Optivity Policy Services (OPS) is network-management software that enables the network administrator to prioritize and manage different types of network traffic. OPS 2.0 is designed to manage policies on the BPS and Business Communication Server (BCM). To manage BayRS, Accelar, and Passport devices, OPS 1.1.1 must be installed.

See "DHCP supplemental information" on page 279 for configuration examples.

Bandwidth Management

This section provides an overview of how the Bandwidth Management feature works, and is useful when considering how to engineer a network of Call Servers. For additional information on the detailed configuration of Bandwidth Management, refer to the following:

- *IP Peer Networking: Installation and Configuration* (553-3001-213)
- *Branch Office: Installation and Configuration* (553-3001-214)
- *Main Office Configuration for the Survivable Remote Gateway 50: Configuration Guide* (553-3001-207)

Bandwidth management provides a means of controlling the amount of Voice over IP (VoIP) traffic in an IP network. Call Servers in the network keep track of the various amounts of VoIP traffic and provide treatment to VoIP calls. Treatment may consist of blocking new calls (Call Admission Control) or rerouting them if there is not the required bandwidth available. For example, when a caller attempts to make a VoIP call and the bandwidth limit has been reached, the call is blocked or rerouted.

Bandwidth Management also allows for a particular CODEC to be selected depending on the type of call — whether it is a local call within the LAN or a remote call across a WAN.

Bandwidth Management is considered a QoS mechanism because it provides a means of guaranteeing that VoIP traffic does not use more network bandwidth than is available.

Bandwidth Management Zones simplify VoIP network voice engineering. Bandwidth Management Zones allow an administrator to simply enter the amount of bandwidth available for voice on the IP network, instead of detailed voice CCS calculations across a particular link.

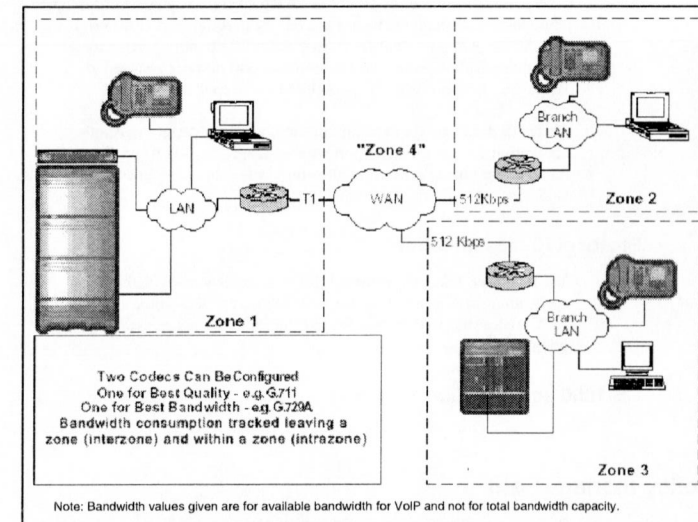
For example, if a CCS-type approach to VoIP network voice engineering is used, an administrator must calculate the maximum CCS expected between sites A to B, A to C, and B to C, and subsequently engineer the network to support the required call volume.

Alternatively, through the use of Bandwidth Management Zones, an administrator may enter the amount of bandwidth available for voice on the IP network into the Call Server. The amount of bandwidth is ensured using other QoS mechanisms, such as priority, as well as the type of voice CODEC that is used. The Call Server then ensures that the VoIP call volume entering or leaving a zone does not exceed the IP network bandwidth available. This enables users to avoid quality degradation because of insufficient bandwidth for active connections.

Call admission control applies equally well to a single distributed system with centralized call control, or multiple systems, as in the case of a main site with numerous branch offices connected with VoIP.

Figure 16 on page 84 shows an example of Bandwidth Management.

Figure 16
Bandwidth management example



VoIP bandwidth management zones

Bandwidth management zones divide IP Phones and Voice Gateway Media Cards into logical groupings (zones) to determine CODEC selection and bandwidth management. Zones are configured after the QoS-managed IP network has been designed.

As calls are made, the Call Server software chooses a CODEC to be used for the call based on the zone configuration (interzone or intrazone). The software also tracks bandwidth usage within each zone and between zones. When making an interzone call, the lowest bandwidth CODEC (BB - Best Bandwidth) between the zones is always chosen.

Each IP Phone and Voice Gateway Media Card port is assigned a zone number in which it resides. Place all IP Phones and Voice Gateway Media Cards at a site in the same zone (for example, set up IP Phones and Voice Gateway Media Cards at the same branch office to be in the same Media Gateway 1000B [MG 1000B] zone).

Virtual Trunk routes also allow configuration of a zone. A single Call Server considers calls out from a Virtual Trunk to be terminated on that Virtual Trunk. Therefore, Virtual Trunks should not be in the same zones as any IP Phones or Voice Gateway Media Cards.

Place all virtual trunk routes in the same zone for all main office and MG 1000B systems. Virtual trunk zones are not for bandwidth management except when connecting to a third-party gateway. Set virtual trunk intrazone and interzone CODECs to Best Quality (BQ). Set virtual trunk intrazone and interzone bandwidth to the maximum value of 1 Gbps (1 000 000 Kbps). Bandwidth is already managed within the IP Phone zone.

Zones are network-wide, therefore zone numbers must not be duplicated. If zone numbers are duplicated on different systems, a call may appear to be an intrazone call. The network-wide zone number is the "vpni" plus the bandwidth zone number. Ensure "vpni" in the customer data block is set to the same value on all systems within the same network (for example, main office or MG 1000B groupings). Calls between two systems with different vpni's are treated as interzone calls.

MG 1000B zones should be configured on the MG 1000B and main office systems. The MG 1000B zones only contain equipment located at that branch office. The information configured for the zone should be identical in both the main and MG 1000B configuration. Main office zone information does not have to be entered into all MG 1000Bs.

Zone properties are defined in LD 117. A maximum of 256 zones can be configured. The systems use the zones for bandwidth management. New calls are blocked when the bandwidth limit is reached.

Each zone has six parameters. The prompt lists the parameters as:

- p1— The total bandwidth available for intrazone calls

- p2 — The preferred strategy for the choice of CODEC for intrazone calls (that is, preserve best quality or best bandwidth)
- p3 — The total bandwidth available for interzone calls
- p4 — The preferred strategy for the choice of the CODEC for interzone calls
- p5 — The zone intent, whether the zone will be part of the main office, a branch office (Media Gateway 1000B [MG 1000B]), or a Virtual Trunk.
- p6 — The zone resource type, either shared or private. Resources in private zones are accessible to users in the same zone. This allows resources, such as DSPs, to be reserved for users in the private zone.

The intrazone and interzone bandwidth is entered in Kbps (for example, 2.7 Mbps equals 2700 Kbps). Each bandwidth zone must have the intrazone and interzone bandwidth values entered.

If no IP voice zones are configured, zone 0 operates as a default zone. If no IP voice zones are configured in LD 117, zone 0 can be configured for ITG Physical TNs (IPTN) in LD 14, and for virtual line in LD 11 as a default zone. However, if any additional zones are required, zone 0 must be first configured in LD 117 if it is referenced by any IP Phone or IPTN. If zone 0 is not configured first, then all calls in zone 0 are labeled as soon as another zone is configured in LD 117.

**CAUTION**

When moving an IP Phone, the system administrator should check and change, if necessary, the zone assignment of the telephone in LD 11. See *Software Input/Output: Administration* (553-3001-311).

**CAUTION**

Zone 0 must be configured in LD 117 before other zones are configured or all calls associated with zone 0 are blocked.

Configuring endpoints in bandwidth zone 0 is not a supported configuration. Configure zone 0, but do not use it. Ensure that no endpoints (for example, IP Phones, VGWs, or vrks) are in zone 0.

Interzone vs. Intrazone

For Bandwidth Management, a network of Call Servers is divided into zones, typically one zone for each Call Server. Calls between zones are known as interzone calls. Calls within a zone are intrazone calls. Typically, intrazone calls travel over LANs on which bandwidth is widely available. Conversely, interzone calls travel over WANs on which bandwidth can be limited and expensive. Differentiating intrazone and interzone VoIP calls allows for increased control over the VoIP traffic.

The following call scenarios describe how each call type works.

Intrazone call

An intrazone call works as follows:

- An intrazone call is made between two endpoints on the same Call Server.
- The intrazone treatment is consulted to determine whether it is Best Bandwidth or Best Quality.
- Based on the intrazone treatment, the correct codec is selected.
- The intrazone bandwidth table is also consulted to determine if there is enough intrazone bandwidth to support the call. If there is not enough bandwidth, the call is blocked.

Interzone call

An interzone call works as follows:

- An intrazone call is made between an endpoint in one zone to another endpoint in a different zone. The zone of the endpoints are compared to the Virtual Trunk zone. Since the two zones are different, the call is an interzone call.
- The interzone treatment is consulted to determine whether it is Best Bandwidth or Best Quality.

- Based on the interzone treatment, the correct codec list is selected for the call setup. See "CODEC selection" on page 90 for more information on codec selection.
- The interzone bandwidth table and the virtual trunk bandwidth limit are also consulted to determine if there is enough intrazone bandwidth to support the call. If there is not enough bandwidth, the call is blocked, or alternate treatment is provided.

Bandwidth Management is nodal

Bandwidth Management is controlled independently on each Call Server in the network. This means that each Call Server acts independently of other Call Servers in the network when calculating bandwidth used, and when blocking or re-routing calls. This is called "nodal" Bandwidth Management — each node, or Call Server, independently controls the Bandwidth Management. Therefore, the parameters used in configuring Bandwidth Management must be configured on each Call Server.

The exception to this rule is at the branch office. The Bandwidth Management at the branch office is controlled by the associated main office. For the main office to keep track of the bandwidth going to and from the branch office, calls must be tandemed through the main office Call Server. This means that the signaling for the call goes through the main office but the media path is not direct between endpoints.

VPNI and Zone numbers

Bandwidth Zone

In order for bandwidth management to work correctly in a CS1000 network, each Call Server must be configured with a unique Network Bandwidth Zone. There are 256 (0-255) Zone numbers available to choose from in a CS1000 Call Server. To allow the network to expand beyond the 256 zones, the Virtual Private Network Identifier (VPNI) is combined with the Zone number to form a unique Network Bandwidth Zone. The CS1000 system allows for up to 16283 VPNI which results in a total of 4,152,165 unique Network Bandwidth Zones. A Call Server typically has one VPNI and one Zone number for IP Phones and IP gateways. For example, Call Server A is provisioned with VPNI 53 and zone 21.

VPNI and Zone numbering rules

Bandwidth Zones are network-wide therefore Bandwidth Zone numbers must not be duplicated at different Call Servers. If these numbers are duplicated on different systems, a call can appear to be an intrazone call. To ensure uniqueness and correct functionality, every main office Call Server in the network must have a unique VPNI.

Branch office Call Servers associated with a main office must have the same VPNI number as the main office. This allows for the correct operation of the Network Bandwidth Management feature.

For a branch office associated with a main office, the branch office Zone number must be different than the main office Zone number. For example, the following is an acceptable configuration: MO VPNI=22, MO Zone=33, BO VPNI=22, BO Zone=34. The branch office zone number is provisioned at both the branch office and the main office. These are configured in LD 117 on the main office and MG1000B.

The provisioned Zone number is also used for other features in the CS 1000 network. See *Emergency Services Access: Description and Administration* (553-3001-313).

Disabling Bandwidth Management

Bandwidth Management may be disabled by provisioning the VPNI = 0 in LD 15 and setting the Zone = 0 on all the endpoints (telephones and Voice Gateway Media Cards). In addition, provision the Virtual Trunks with Zone = 0.

Provision the Intrazone bandwidth limit and Interzone bandwidth to the maximum (1 Gbps or 1 000 000 Kbps) in LD 117.

Nortel recommends that customers not mix enabled and disabled Bandwidth Management zones in the network.

Relationship between zones and subnets

IP Phones and Voice Gateway Media Cards gateway ports are assigned to zones based on the bandwidth management requirements of the particular installation. Devices in different subnets must traverse a router to communicate and can reside on different ends of a WAN facility. When IP Phones and gateway ports are in different subnets, the network facilities between them must be examined to see if it warrants placing the separated devices in different zones.

It is not necessary to always assign different zones. For instance, there can be different subnets within a LAN interconnected by router(s) with sufficient bandwidth. The IP Phones and gateway channels spread across them could all reside in a single zone. However, if there is a WAN facility with limited bandwidth between two subnets, the devices on the opposite ends should be placed in different zones so the bandwidth across the WAN can be managed.

For remote users such as telecommuters, bandwidth management is not normally a consideration because only one IP Phone is present at the remote location. It can be convenient to allocate zones for users with similar connection speeds. In that case, set both the interzone and intrazone CODEC to Best Bandwidth.

Adaptive Bandwidth Management

Adaptive Bandwidth Management (ADBWM) applies only to Interzone traffic. Adaptive bandwidth management builds on Bandwidth Management but adds two new functionalities. The first is that adaptive bandwidth management automatically changes the bandwidth limit depending upon the Quality of Service (QoS) in the network. The second is that the bandwidth limit is automatically adjusted on a zone-to-zone basis. So if there are QoS problems reported between a Call Server in zone 3 and another in zone 5 then the bandwidth limit is reduced for calls between zone 3 and zone 5.

CODEC selection

To ensure optimal voice quality, minimize the number of compression and decompression stages and wherever bandwidth permits, use a G.711 CODEC.

The Call Server considers BQ to be G.711 and BB to be either G.729 or G.723.

Each CODEC has specific parameters that must be configured, such as packetization delay and voice activity detect. These parameters are configured on the Signaling Server using Element Manager. For further information, see "Element Manager" on page 222.

Ensure the voice CODEC images on all sites match. The simplest way to ensure this is through the use of the same software version at each site. Use the same CODECs, packetization and jitter buffer settings on each system.

There is a potential to degrade the voice quality if CODECs are cascaded. This can occur when there are multiple compression and decompression stages on a voice call. The more IP links used in a call, the more delay is added, and the greater the impact on voice quality.

The following applications and devices can impact voice quality if you use a compression CODEC such as G.729A:

- Voice mail, such as Nortel CallPilot, introduces another stage of compression and decompression.
- Conferences can double the number of IP links.
- IP Trunks can add additional stages of compression and decompression.

Note: Nortel recommends that all cards in a system have the same image. If multiple CODEC images are used in an VoIP network, the calls default to the G.711 group when the originating and destination CODECs are different.

For additional information on CODECs, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

VoIP network voice engineering considerations

It may be necessary to calculate CCS between zones to determine if the network can support the required call volume.

For more information refer to:

- "Bandwidth" on page 110
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)

Determining interzone and intrazone bandwidth values

The Call Server uses the values shown in Table 6 when calculating the bandwidth each call uses in a zone. The Call Server uses the values in the "TLAN Bandwidth" columns and subtracts the value from the available zone bandwidth to determine if a zone has sufficient bandwidth for the call.

Table 6
Bandwidth estimates used by Call Admission Control (Part 1 of 2)

CODEC type	Packet duration (ms)	Voice payload (bytes)	VAD	TLAN Bandwidth (half-duplex, payload/RTP/UDP/IP/Ethernet)		Base WAN Bandwidth (full-duplex, payload/RTP/UDP/IP)	
				Peak bandwidth (Kbps)	Average bandwidth (Kbps)	Peak bandwidth (Kbps)	Average bandwidth (Kbps)
G.711 (64 Kbps)	10	80	Off	252.80	252.80	96.00	96.00
	20	160	Off	190.40	190.40	80.00	80.00
	30	240	Off	169.60	169.60	74.67	74.67
G.729A (8 Kbps)	10	10	Off	140.80	140.80	40.00	40.00
	20	20	Off	78.40	78.40	24.00	24.00
	30	30	Off	57.60	57.60	18.67	18.67
	40	40	Off	47.20	47.20	16.00	16.00
	50	50	Off	40.96	40.96	14.40	14.40

Table 6
Bandwidth estimates used by Call Admission Control (Part 2 of 2)

CODEC type	Packet duration (ms)	Voice payload (bytes)	VAD	TLAN Bandwidth (half-duplex, payload/RTP/UDP/IP/Ethernet)		Base WAN Bandwidth (full-duplex, payload/RTP/UDP/IP)	
				Peak bandwidth (Kbps)	Average bandwidth (Kbps)	Peak bandwidth (Kbps)	Average bandwidth (Kbps)
G.729AB (8 Kbps)	10	10	On	140.80	84.48	40.00	24.00
	20	20	On	78.40	47.04	24.00	14.40
	30	30	On	57.60	34.56	18.67	11.20
	40	40	On	47.20	28.32	16.00	9.60
	50	50	On	40.96	24.58	14.40	8.64
G.723.1 (6.3 Kbps)	30	24	Off	54.40	54.40	17.07	17.07
G.723.1 (5.3 Kbps)	30	24	Off	54.40	54.40	17.07	17.07

The TLAN Bandwidth values contain the total IP and Ethernet packet overhead of 78 bytes, including the 8-byte preamble and minimum 12-byte inter-packet gap. These are often excluded from bandwidth calculations but must be included to give a true indication of the bandwidth used. The Call Server assumes that all calls are made over a half-duplex Ethernet network.

Note: The Call Server is unaware of the particulars of the WAN facility and always uses the values shown in the TLAN Bandwidth columns.

The columns labeled Base WAN Bandwidth provide the data for the payload plus IP overhead without the Ethernet interface overhead. This data provides the basis for any WAN bandwidth calculations. The overhead associated with the particular WAN facility (for example, Frame Relay) is added to the base value to determine the total bandwidth used. The values shown are for a half-duplex link, so if the WAN facility is half-duplex, the values should be doubled. This should be considered when entering the intrazone and interzone bandwidth values for a zone in LD 117.

The IP/UDP/RTP header size is 40 bytes.

Procedure 3 describes the simplest way to calculate the bandwidth amount to be entered into the bandwidth zones table.

Procedure 3
Calculating bandwidth amount for bandwidth zones table

- 1 Determine the number of calls that the network can actually support for the chosen CODEC.
- 2 Multiply the half-duplex Ethernet bandwidth by the value determined in step 1.
- 3 Enter the value determined in step 2 in the Call Server bandwidth zone table.

End of Procedure

Ensure that the efficiency of the network transporting VoIP is taken into account when entering the amount of zone bandwidth available. Refer to the efficiency example in "Bandwidth and data network switch efficiency" on page 35.

Follow the steps in Procedure 4 to determine intrazone bandwidth.

Procedure 4
Determining intrazone bandwidth

- 1 Determine the VoIP CODEC and packet duration to be used for interzone calls.
- 2 Determine the network duplex, Layer 2 protocol, and Layer 2 protocol header size between zones.
- 3 Determine the total bandwidth available for voice on the data network.
- 4 Calculate the per-call bandwidth use for the CODEC (from step 1) over the Layer 2 network (from step 2).

Per-call bandwidth for a particular Layer 2 network:
 $(1000 / \text{Packet Duration [ms]}) \times (\text{Voice payload Bytes}) + \text{IP / UDP / RTP Size (Bytes)} + \text{Layer two Protocol Header Size [Bytes]} \times 8$

Alternatively, see See "VoIP Bandwidth Demand Calculator" on page 117.

- 5 Calculate the number of calls the network is actually capable of handling. To do this, divide the total bandwidth available for voice over the Layer 2 network (from step 3) by the real per-call bandwidth use for the CODEC (from step 4).
- 6 Determine the half-duplex Ethernet bandwidth for one call for the CODEC (from step 1) to be used. See Table on page 92.
- 7 Calculate the bandwidth value to enter into the Call Server bandwidth management zone. Multiply the half-duplex Ethernet bandwidth (from step 6) by the number of calls the network is actually capable of handling.

End of Procedure

Determination of intrazone bandwidth is not normally required. This is because a large amount of bandwidth is normally available within a local network, so an arbitrarily large value can be entered for the interzone bandwidth available.

If required, interzone bandwidth is calculated using the same procedure as for intrazone bandwidth (see Procedure 4 on page 94).

Example: Interzone bandwidth calculation

Based on Bandwidth management of G.729A interzone traffic over a 512-Kbps Frame Relay network, as shown in Figure 16 on page 84, perform the following steps:

- 1 CODEC = G.729A, 20ms
- 2 Network type = Full duplex Frame Relay with 6-byte header
- 3 Total bandwidth available = $512 \text{ Kbps} \times 0.9 = 460.8 \text{ Kbps}$ (0.9 is an estimate of the efficiency of a random Frame Relay router. The actual efficiency may vary. See calculating data network switch efficiency in "Bandwidth and data network switch efficiency" on page 35)

- 4 G.729A per-call bandwidth on a full duplex frame relay network
 $= (1000 / 20) \times (20 + 40 + 6) \times 8 = 26400 \text{ bps} = 26.4 \text{ Kbps}$
- 5 Total calls possible = $460.8 \text{ Kbps} / 26.4 \text{ kbps} = 17 \text{ calls}$
- 6 G.729A half-duplex Ethernet per-call bandwidth = 78.4 Kbps
- 7 Call Server bandwidth value = $78.4 \text{ Kbps} \times 17 \text{ calls} = 1333 \text{ Kbps}$

Therefore, enter 1333 Kbps in the Call Server.

Viewing bandwidth statistics

Use the PRT INTRAZONE and PRT INTERZONE commands in LD 117 to display the bandwidth statistics in the Call Server. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) or *Software Input/Output: Maintenance* (553-3001-511) for more information on these commands. See Figure 17 on page 96 and Figure 18 on page 97 for examples of the output of these commands.

Figure 17
Sample output for PRT INTRAZONE command

```
=> prt intrazone
```

Zone	State	Type	Strategy	MO/	Bandwidth	Usage	Peak
				BMG/	kbps	kbps	%
				VTRK			
2	ENL	SHARED	BQ	MO	10000	190	3
44	ENL	SHARED	BQ	BMG	10000	0	1

Number of Zones configured = 2

Figure 18
Sample output for PRT INTERZONE command

-> prt interzone

Near end		Far end		State	Type	Strategy	MO/BMG/VTRK	QoS Factor	Bandwidth Configured	Sliding max	Usage	Peak	Calls	Alarm
Zone	VPNI	Zone	VPNI					%	kbps	kbps	kbps	%	Cph	Aph
2				ENL	SHARED	BB	MO		10000		78	1		
2	1	33	1	ENL	SHARED	BB	MO	100	10000		78	1	1	0
33				ENL	SHARED	BB	BMG		10000		78	1		
33	1	2	1	ENL	SHARED	BB	BMG	100	10000		78	1	1	0

Number of Zones configured = 1

Note: The Far end and VPNI fields are displayed only when Adaptive Bandwidth Management is enabled in LD 117.

Network performance measurement

Contents

This section contains information on the following topics:

Introduction	100
Performance criteria	101
Network performance evaluation overview	102
Network performance measurement tools	108
Network availability	109
Bandwidth	110
Available Bandwidth	110
Guaranteed Bandwidth	110
Queueing	111
Calculating per-call bandwidth use	111
Silence Suppression engineering considerations	117
Estimate network loading caused by VoIP traffic	118
Route Link Traffic estimation	123
Enough capacity	124
Insufficient link capacity	126
Other intranet resource considerations	126
Delay	126
Effects of delay on voice quality	129
Components of delay	129
Measuring end-to-end network delay	133
Adjusting PING statistics	135
Other measurement considerations	136
Reducing delays	136

Reducing hop count	137
Recording routes	137
Routing issues	138
Jitter	138
Jitter buffers	140
Late packets	140
Adjusting jitter buffer size	141
Jitter measurement tools	142
Packet loss	143
Physical medium loss	143
Congestion loss	143
Measuring end-to-end packet loss	145
Packet Loss Concealment	145
Reducing packet loss	146
Network delay and packet loss evaluation example	147
Estimate voice quality	148
Sample scenarios	152
Does the intranet provide expected voice quality?	154

Introduction

To create a VoIP-grade network, certain QoS standards for basic network elements must be met. The following QoS parameters can be measured and monitored to determine if desired service levels have been obtained:

- network availability
- bandwidth
- delay
- jitter
- packet loss

These QoS parameters and mechanisms affect the application's or end-user's Quality of Experience (QoE). These QoS parameters apply to any IP network carrying VoIP traffic, including LANs, campus-wide networks, and WANs.

Performance criteria

This section describes criteria for achieving excellent voice quality. The network should meet these specifications.

- **End-to-end packet delay:** Packet delay is the point-to-point, one-way delay between the time a packet is sent to the time it is received at the remote end. It is comprised of delays at the Voice Gateway Media Card, Internet Telephone, and the IP network. To minimize delays, the IP Telephony node and Internet Telephone must be located to minimize the number of hops to the network backbone or WAN.

Note: Nortel recommends an end-to-end delay of ≤ 50 ms on the IP network to ensure good voice quality. This does not include the built-in delay of the Voice Gateway Media Card and IP Phone.

- **End-to-end packet loss:** Packet loss is the percentage of packets sent that do not arrive at their destination. Transmission equipment problems, packet delay, and network congestion cause packet loss. In voice conversation, packet loss appears as gaps in the conversation. Sporadic loss of a few packets can be more tolerable than infrequent loss of a large number of packets clustered together.

Note: For high-quality voice transmission, the long-term average packet loss between the IP Phones and the Voice Gateway Media Card TLAN network interface must be $< 1\%$, and the short-term packet loss must not exceed 5% in any 10-second interval.

Recommendation

To achieve excellent voice quality, Nortel strongly recommends using G.711 CODEC with the following configuration:

- end-to-end delay less than 150 ms one way (network delay + packetization delay + jitter buffer delay < 150). See "IP expansion link Packet Delay Variation jitter buffer" on page 207.
- packet loss less than 0.5% (approaching 0%)
- maximum jitter buffer setting for IP Phone as low as possible (maximum 100 ms)

Packet loss on the ELAN network interface can cause:

- communication problems between the Call Server and the Voice Gateway Media Cards
- lost SNMP alarms
- incorrect status information on the OTM console
- other signaling-related problems

Note: Since the ELAN network is a Layer 2 Switched LAN, the packet loss must be zero. If packet loss is experienced, its source must be investigated and eliminated. For reliable signaling communication on the ELAN network interface, the packet loss must be $< 1\%$.

Network performance evaluation overview

There are two main objectives when dealing with the QoS issue in an IP network:

- 1 Predict the expected QoS.
- 2 Evaluate the QoS after integrating VoIP traffic into the intranet.

The process for either case is similar—the first is without VoIP traffic, and the second is with VoIP traffic. The differences are discussed in this section.

Procedure 5 Evaluating network performance – overview

This process assumes that the PING program is available on a PC, or some network management tool is available to collect delay and loss data and to access the LAN that connects to the router to the intranet.

- 1 Use PING or an equivalent tool to collect round-trip delay (in ms) and loss (in%) data.
- 2 Divide the delay (determined in step 1) by 2 to approximate one-way delay. Add 93 ms to adjust for ITG processing and buffering time.
- 3 Use a QoS chart, or Table 20 on page 151, to predict the QoS categories: Excellent, Good, Fair or Poor.

- 4 If a customer wants to manage the QoS in a more detailed fashion, re-balance the values of delay compared to loss by adjusting system parameters, such as preferred CODEC, payload size, and routing algorithm, to move resulting QoS among different categories.
- 5 If the QoS objective is met, repeat the process periodically to make sure the required QoS is maintained.

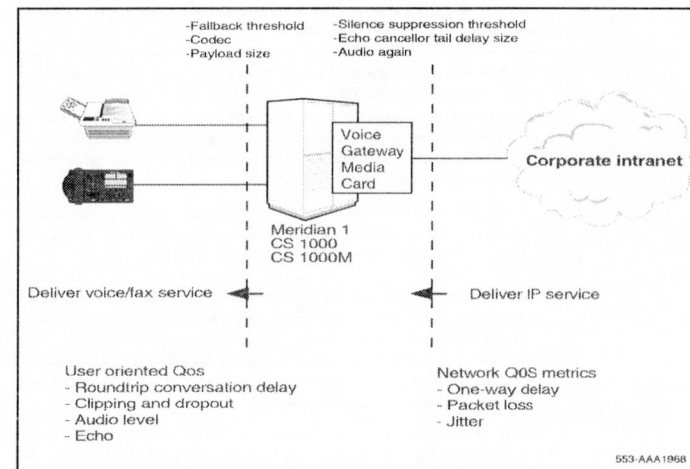
End of Procedure

Set QoS expectations

The users of corporate voice and data services expect these services to meet some perceived Quality of Service (QoS) which in turn influences network design. The goal is to design and allocate enough resources in the network to meet users' needs. QoS metrics or parameters are what quantifies the needs of the "user" of the "service".

In the context of a Meridian 1, CS 1000S, and CS 1000M system, Figure 19 on page 104 shows the relationship between users and services.

Figure 19
QoS parameters



In Figure 19, there are two interfaces to consider.

- The Meridian 1, including the IP Trunk 3.0 (or later) nodes, interfaces with the end users. Voice services offered by the Meridian 1 must meet user-oriented QoS objectives.
- The IP Trunk 3.0 (or later) nodes interface with the intranet. The service provided by the intranet is "best-effort delivery of IP packets", not "guarantee QoS for real-time voice transport." IP Trunk 3.0 (or later) translates the QoS objectives set by the end-users into IP-oriented QoS objectives. The guidelines call these objectives *intranet QoS objectives*.

The QoS level is a user-oriented QoS metric which takes on one of four settings – Excellent, Good, Fair, or Poor – indicating the quality of voice

service. IP Trunk 3.0 (or later) periodically calculates the prevailing QoS level per site pair, based on its measurement of the following:

- one-way delay
- packet loss
- CODEC

Recommendation

Nortel strongly recommends that G.711 CODEC be used over high-bandwidth connections, and used any time that call quality is the highest priority. Where call quality is the highest priority, sufficient bandwidth must be provided for the VoIP application. The Best Quality (BQ) CODEC is usually chosen and configured as G.711 within the zone configuration (intrazone).

Use G.729 CODEC to compress voice traffic over low-bandwidth connections when bandwidth considerations take precedence over call quality. The Best Bandwidth (BB) CODEC is usually chosen and set to G.729A or G.729AB between zones (interzone).

CODEC details are then configured on the Signaling Server through OTM or CS 1000 Element Manager.

Figure 20 on page 106, Figure 21 on page 107, and Figure 22 on page 108 are derived from the ITU-T G.107 Transmission Rating Model. These diagrams show the operating regions in terms of *one-way delay* and *packet loss* for each CODEC. Note that among the CODECs, G.711 A-law/G.711 mu-law delivers the best quality for a given intranet QoS, followed by G.729AB, G.723.1 6.4 kbps, and G.723.1 5.3 kbps. These graphs determine the delay and error budget for the underlying intranet so it delivers a required quality of voice service.

Fax is more susceptible to packet loss than is the human ear, in that quality starts to degrade when packet loss exceeds 4%. Nortel recommends that fax services be supported with IP Trunk 3.0 (or later) operating at the Excellent or Good QoS level. Avoid offering fax services between two sites that can guarantee no better than a Fair or Poor QoS level.

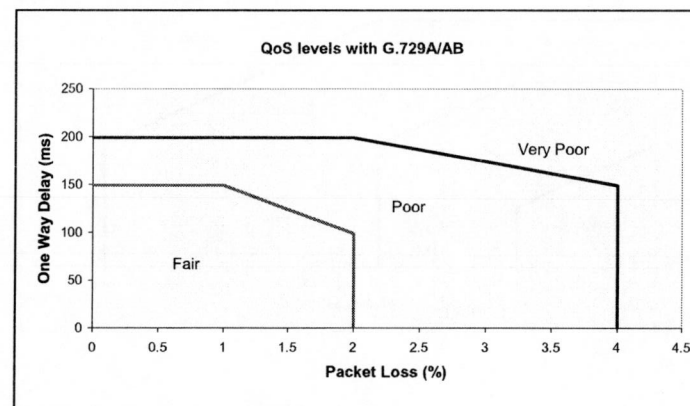
G.729AB CODEC

The G.729 uses less bandwidth than the G.711. If minimizing bandwidth demand is a priority, and the customer is willing to accept lesser voice quality, a G.729AB CODEC can be used.

Extreme care must be taken in the network design if using the G.729AB CODEC. The G.729AB CODEC has the same requirements as the G.711 CODEC.

Figure 20 shows the QoS levels with a G.729A/AB CODEC.

Figure 20
QoS levels with G.729A/AB CODEC

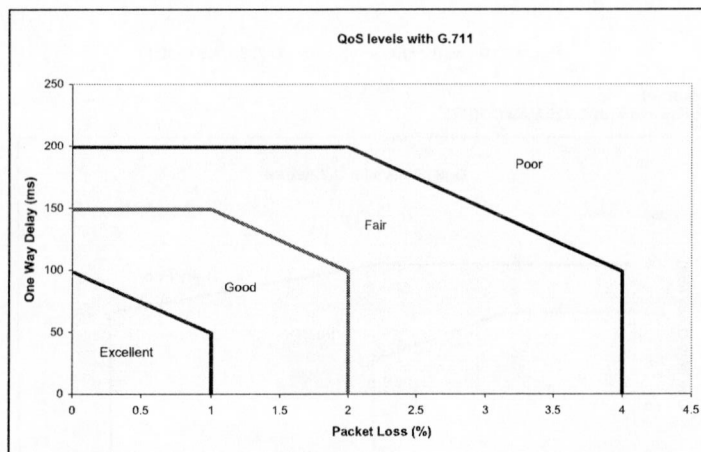


G.711 CODEC

G.711 is the recommended CODEC.

Figure 21 shows the QoS levels with a G.711 CODEC.

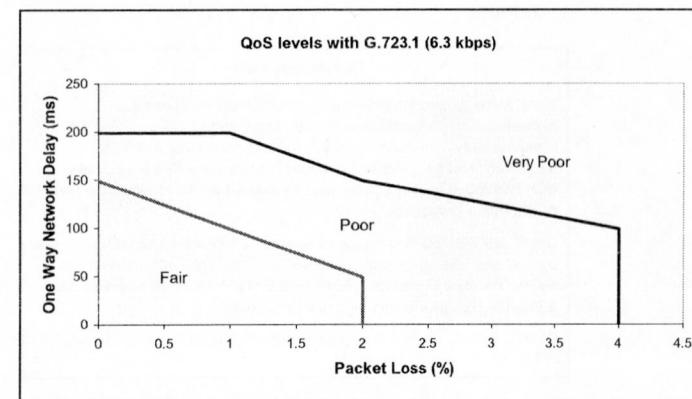
Figure 21
QoS level with G.711 CODEC



G.723 CODEC

Figure 22 shows the QoS levels with a G.723 CODEC.

Figure 22
QoS level with G.723 CODEC



Network performance measurement tools

PING and Traceroute are standard IP tools that are usually included with a network host's TCP/IP stack. QoS measurement tools and packages are commonly available. They include delay monitoring tools that include features like timestamping, plotting, and computation of standard deviation. For information on network performance measurement tools, refer to:

- "QoS monitoring and reporting tools" on page 228
- "Proactive Voice Quality Management" on page 241
- *IP Phones: Description, Installation, and Operation* (553-3001-368)

The following measuring tools are based on the Internet Control Messaging Protocol (ICMP):

- PING — sends ICMP echo requests
- Traceroute — sends packets to unequipped port numbers and processes to create ICMP destination unavailable messages

Both PING and Traceroute are basic measuring tools that can be used to assess the IP Line network. They are standard utilities that come with most commercial operating systems. PING is used to measure the round-trip delay of a packet and the percentage of packet loss. Traceroute breaks down delay segments of a source-destination pair and any hops in-between to accumulate measurements.

There are several third-party applications that perform data collection similar to PING and Traceroute. In addition, these programs analyze data and plot performance charts. The use of PING and Traceroute to collect data for manual analysis is labor intensive; however, they provide information as useful as the more sophisticated applications.

Network availability

Network availability has the most significant effect on QoS. If the network is unavailable, even for brief periods of time, the user or application can achieve unpredictable or undesirable performance levels.

Network availability is dependent on the availability of a survivable, redundant network. A redundant network should include the following elements to ensure survivability:

- redundant devices such as
 - interfaces
 - processor cards
 - power supplies in routers and switches
- resilient networking protocols
- multiple physical connections, such as copper or fiber
- backup power sources

Network availability has the most significant effect on QoS. If the network is unavailable, even for brief periods of time, the user or application can achieve unpredictable or undesirable performance levels.

It is necessary to engineer a survivable network to provide guaranteed network availability.

Bandwidth

Bandwidth is the most significant parameter that affects QoS. There are two types of bandwidth:

- Available Bandwidth
- Guaranteed Bandwidth

IMPORTANT!

The use of QoS mechanisms that prioritize voice over data traffic effectively increases the amount of bandwidth available to voice traffic.

Available Bandwidth

Many network operators oversubscribe the bandwidth on their network to maximize the return on their network infrastructure or leased bandwidth.

Oversubscribing bandwidth means that the bandwidth a user subscribes to is not always available. All users compete for Available Bandwidth. The amount of bandwidth available to a user depends on the amount of traffic from other network users at any given time.

Guaranteed Bandwidth

Some network operators offer a service that guarantees a minimum bandwidth and burst bandwidth in the Service Level Agreement (SLA). This service is more expensive than the Available Bandwidth service. The network operator must ensure that the Guaranteed Bandwidth subscribers get preferential treatment (QoS bandwidth guarantee) over the Available Bandwidth subscribers.

This can be accomplished in several ways. Sometimes, the network operator separates the subscribers by different physical or logical networks, such as Virtual Local Area Networks (VLANs) or Virtual Circuits.

In other cases, the Guaranteed Bandwidth traffic shares the same infrastructure as the Available Bandwidth traffic. This is often seen where network connections are expensive, or where the bandwidth is leased from other service providers. When both types of subscribers share the same infrastructure, the network must prioritize Guaranteed Bandwidth traffic over Available Bandwidth traffic. This ensures that when network traffic is heavy, the Guaranteed Bandwidth subscriber's SLA is met.

Queueing

Over-engineering network bandwidth does not necessarily solve voice quality problems, as IP network traffic is inherently bursty in nature. At any time, a burst of packets can enter a switch. If the number of packets received in that instant is greater than the capacity of the transmitting port's queue, then packets are lost. This situation is particularly serious on slow connections.

If a queue is busy (though not necessarily full), voice packet traffic can back up and jitter can occur if voice packets are not prioritized. Network QoS mechanisms are based on assigning different priorities to multiple queues. A voice queue is assigned a higher priority. If a specific queue is assigned only to voice traffic, then there is less chance that voice packets will be discarded because the queue is too full. Network delay is reduced, as voice packets are transmitted first. This minimizes delay, jitter, and loss. Perceived voice quality is greatly improved.

Calculating per-call bandwidth use

Calculating VoIP traffic requirements

It is necessary to forecast the hundreds of call seconds for each hour (CCS) of traffic that the CS 1000 and Meridian 1 systems processes through the IP Line network. CCS traffic generated by an IP Phone is similar to that of a digital telephone. The procedures in the section calculate the bandwidth required to support given amounts of traffic.

The procedures require the:

- CCS/CCS rating of IP Phone
- For more information, refer to *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120).

- number of IP Phones
- number of subnets/servers accessed by the IP Phones

Note: Base all traffic data on busy hour requirements.

The result of the calculation provides estimated values of the following requirements:

- total LAN bandwidth requirement
- WAN bandwidth requirement for each subnet or server/router

It is necessary to consider the impact of incremental IP Line traffic on routers and LAN resources in the intranet. LAN segments can become saturated, and routers can experience high CPU use. Consider re-routing scenarios in a case where a link is down.

Calculating LAN traffic

To calculate the total LAN requirement, total all sources of traffic destined for the Internet Telephony network using the same LAN. The data rate for a LAN is the total bit rate. The total subnet traffic is measured in Erlangs. An Erlang is a telecommunications traffic measurement unit used to describe the total traffic volume of one hour. Network designers use these measurements to track network traffic patterns.

Follow the steps in Procedure 6 on page 113 to calculate the LAN traffic.

Procedure 6 Calculating LAN traffic

- 1 Add the following to calculate total subnet traffic (in Erlangs):

- number of IP Phones $\times$ (CCS $\div$ CCS rating)
- voice gateways on Voice Gateway Media Card
- WAN connection

Note: Each source of traffic has a different CCS rating. Calculate the subnet traffic for each source of traffic and add the amounts to get the total.

- 2 Use the number of Erlangs to calculate the equivalent number of lines by using the calculator at the following website:

<http://www.erlang.com/calculator/erlb>

Assume a blocking factor of 1% (0.010).

- 3 Find the LAN bandwidth usage (Kbps) in Table 6 on page 92, based on the CODEC used for the traffic source.
- 4 Calculate the bandwidth of a subnet using the following calculation:
Subnet bandwidth = Total number of lines $\times$ LAN bandwidth usage
- 5 Repeat step 1 to step 4 for each subnet.
- 6 Calculate the total LAN traffic by adding the total bandwidth for each subnet calculation.

End of Procedure

LAN engineering example

The following is an example of calculating LAN bandwidth assuming half-duplex links.

Using G.729AB 30 ms, LAN bandwidth usage is 57.6 Kbps.

The formula is:

$$\text{Number of Erlangs} = \text{Number of IP Phones} \times (\text{CCS} \div 36)$$

- 1 Subnet A: 28 Internet Telephones, average 6 CCS $\div$ IP Phone
Subnet A total Erlangs = $28 \times 6 \div 36 = 4.66$
Subnet A bandwidth = $4.66 \times 57.6 \text{ Kbps} = 268.4 \text{ Kbps}$
- 2 Subnet B: 72 IP Phones, average 5 CCS $\div$ Internet Telephone
Subnet B total Erlangs = $72 \times 5 \div 36 = 10$
Subnet B bandwidth = $10 \times 57.6 = 576 \text{ Kbps}$
- 3 Subnet C: 12 IP Phones, average 6 CCS $\div$ IP Phone
Subnet C total Erlangs = $12 \times 6 \div 36 = 2$
Subnet C bandwidth = $2 \times 57.6 = 115.2 \text{ Kbps}$
- 4 Calculate the LAN Bandwidth by finding the sum of all subnet bandwidths:
LAN Bandwidth = $268.4 + 576 + 115.2 = 959.6 \text{ Kbps}$

WAN traffic calculations

For data rate requirements for the intranet route, calculation is based on duplex channels. The data rate for a WAN is the duplex data rate. For example, 128 Kbps on the LAN is equal to a 64 Kbps duplex channel on the WAN. Use the following procedure to calculate data rate requirements for the intranet route. The effects of Real-time Transport Protocol (RTP) header compression by the router are not considered in these calculations but must be included where applicable.

Follow the steps in Procedure 7 to calculate WAN traffic.

Procedure 7
Calculating WAN traffic

- 1 Calculate the total subnet traffic using the following formula:
Total subnet traffic = Number of IP Phones x CCS/Internet Telephone.
- 2 Convert to Erlangs:
Total CCS / 36 (on the half-duplex LAN)
- 3 Find WAN bandwidth usage (Kbps) from the "WAN Base Bandwidth" columns of Table 6 on page 92.
- 4 Calculate bandwidth for each subnet = Total Erlangs x WAN bandwidth usage.
- 5 Multiply bandwidth of each subnet by 1.3 to adjust for traffic peaking.
- 6 Repeat the procedure for each subnet.
- 7 Adjust WAN bandwidth to account for WAN overhead depending on the WAN technology used:
 - ATM (AAL1): multiply subnet bandwidth x 1.20 (9 bytes overhead/44 bytes payload)
 - ATM (AAL5): multiply subnet bandwidth x 1.13 (6 bytes overhead/47 bytes payload)
 - Frame Relay: multiply subnet bandwidth x 1.20 (6 bytes overhead/30 bytes payload – variable payload up to 4096 bytes)

Note: Each WAN link must be engineered to be no more than 80% of its total bandwidth if the bandwidth is 1536 Kbps or higher (T1 rate). If the rate is lower, up to 50% loading on the WAN is recommended.

End of Procedure

WAN engineering example

The following is an example of calculating the WAN bandwidth.

- 1 Subnet A: 36 IP Phones, average 6 CCS/Internet Telephone
 - Total Erlangs = $36 \times 6/36 = 6$
 - For G.729AB 50 ms, WAN bandwidth usage is 14.4 Kbps.
 - Subnet A WAN bandwidth = $14.4 \times 6 = 86.4$ Kbps
 - Subnet A WAN bandwidth with 30% peaking
= 86.4×1.3
= 112.32 Kbps
- 2 Subnet B: 72 IP Phones, average 5 CCS/IP Phone
 - Total Erlangs = $72 \times 5/36 = 10$
 - Subnet B WAN bandwidth = $14.4 \times 10 = 144$ Kbps
 - Subnet B WAN bandwidth with 30% peaking
= 144×1.3
= 187.2 Kbps
- 3 Subnet C: 12 IP Phones, average 6 CCS/IP Phone
 - Total Erlangs = $12 \times 6/36 = 2$
 - Subnet C WAN bandwidth = $14.43 \times 2 = 28.8$ Kbps
 - Subnet C WAN bandwidth with 30% peaking
= 28.8×1.3
= 37.44 Kbps

- 4 If the WAN is known to be an ATM network (AAL1), the estimated bandwidth requirements are:

- Subnet A WAN bandwidth with ATM overhead
= 112.32×1.2
= 134.78 Kbps.
- Subnet B WAN bandwidth with ATM overhead
= 187.2×1.2
= 224.64 Kbps
- Subnet C WAN bandwidth with ATM overhead
= 37.44×1.2
= 44.93 Kbps

Note: Bandwidth values can vary slightly depending on the transport type.

VoIP Bandwidth Demand Calculator

The VoIP Bandwidth Demand Calculator is a Microsoft® Excel-based tool that quickly determines the bandwidth requirements for a given link.

The VoIP Bandwidth Demand Calculator uses the following variables:

- number of trunks
- packetization interval
- CODEC (G.711, G.729, and G.723)
- link type (Frame Relay, PPP, ATM, Ethernet)
- link speed

Ask a Nortel representative for the VoIP Bandwidth Demand Calculator spreadsheet. Use these parameters and the bandwidth calculator to determine the bandwidth requirement for each client.

Silence Suppression engineering considerations

Silence Suppression/Voice Activity Detection (VAD) results in average bandwidth savings over time, not immediately. For normal conversations, Silence Suppression creates a 40% savings in average bandwidth used. For

example, a single G.729AB voice packet will still consume 30 Kbps of bandwidth but the average bandwidth used for the entire call would be approximately 23 Kbps.

Calculate the average bandwidth using the formula:

CODEC bandwidth from Table 6 on page 92 x 0.6

When voice services with multi-channel requirements are extensively used in an VoIP network, such as Conference, Music-on-hold, and Message Broadcasting, additional voice traffic peaks to the IP network are generated due to the simultaneous voice-traffic bursts on multiple channels on the same links.

Estimate network loading caused by VoIP traffic

An efficient VoIP network design requires an understanding of traffic and the underlying network that carries the traffic. To determine the network requirements of the specific system, the technician must perform the steps in Procedure 8 on page 119.

Before bandwidth estimation can begin, obtain the following network data:

- A network topology and routing diagram.
- A list of the sites where the CS 1000 Release 4.5 nodes are to be installed.
- List the sites with VoIP traffic, and the CODEC and frame duration (payload) to be used.
- Obtain the offered traffic in CCS for each site pair; if available, separate voice traffic from fax traffic (fax traffic sent and received).
- In a network with multiple time zones, use the same real-time busy hour varying actual clock hours) at each site that yields the highest overall network traffic. Traffic to a route is the sum of voice traffic plus the larger of one-way fax traffic either sent or received.

Procedure 8**Determining network requirements – overview**

- 1 Estimate the amount of traffic processed by the Meridian 1 or CS 1000 system through the IP Line network.

See *Capacity Engineering* (553-3001-149) and *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120).

- 2 Assess if the existing corporate intranet can adequately support voice services.

See "Network design assessment" on page 27.

- 3 Organize the IP Line network into "zones" representing different topographical areas of the network that are separated according to bandwidth considerations.

- 4 Ensure that appropriate QoS measures are implemented across the network to prioritize voice packets over data traffic.

End of Procedure**Example — multi-node engineering**

Table 7 summarizes traffic flow of a 4-node CS 1000 network.

Table 7

Example: Traffic flow in a 4-node CS 1000 network

Destination Pair	Traffic in CCS
Santa Clara/Richardson	60
Santa Clara/Ottawa	45
Santa Clara/Tokyo	15
Richardson/Ottawa	35
Richardson/Tokyo	20
Ottawa/Tokyo	18

The CODEC selection is on a per-call basis. During call setup negotiation, only the type of CODEC available at both destinations is selected. When no agreeable CODEC is available at both ends, the default CODEC G.711 is used.

For this example, assume that the preferred CODEC to handle VoIP calls in this network is G.729AB.

Table 8 summarizes the WAN traffic in kbit/s for each route. The recommended incremental bandwidth requirement is included in the column adjusted for 30% traffic peaking in busy hour. This assumes no correlation and no synchronization of voice bursts in different simultaneous calls. This assumes some statistical model of granularity and distribution of voice message bursts due to Silence Suppression.

Table 8

Example: Incremental WAN bandwidth requirement

Destination Pair	CCS on WAN	WAN traffic in kbit/s	Peaked WAN traffic (x1.3) in kbit/s
Santa Clara/Richardson	60	18.7	24.3
Santa Clara/Ottawa	45	14.0	18.2
Santa Clara/Tokyo	15	4.7	6.1
Richardson/Ottawa	35	10.9	14.2
Richardson/Tokyo	20	6.2	8.1
Ottawa/Tokyo	18	5.6	7.3

The Santa Clara/Richardson information is calculated as follows:

- The total traffic on this route is 60 CCS. To use the preferred CODEC of G.729AB with a 30 ms payload, the bandwidth on the WAN is 11.2 kbit/s.
- WAN traffic is calculated by: $(60/36) * 11.2 = 18.7$ kbit/s.

- Increasing this number by 30% gives a peak traffic rate of 24.3 kbit/s. This is the incremental bandwidth required between Santa Clara and Richardson to carry the 60 CCS voice traffic during the busy hour.

Assume that 20 CCS of the 60 CCS between Santa Clara and Richardson is fax traffic. Of the 20 CCS, 14 CCS is from Santa Clara to Richardson, and 6 CCS is from Richardson to Santa Clara. What is the WAN data rate required between those two locations?

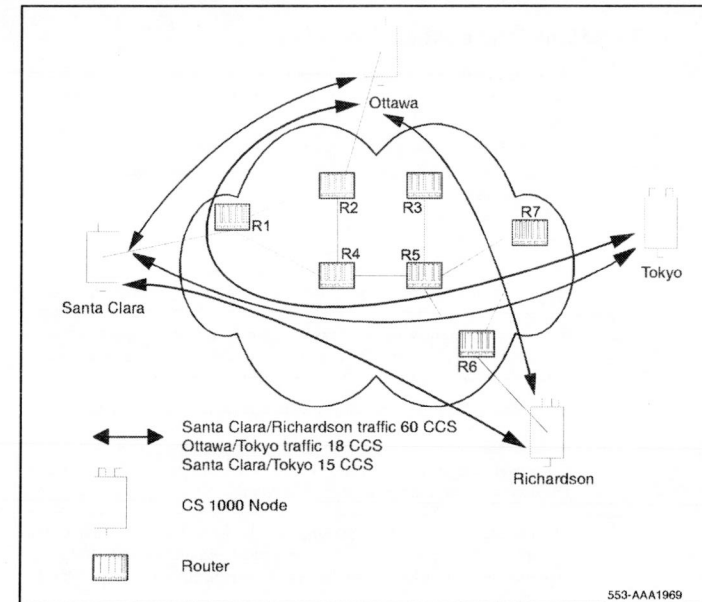
- Traffic between the two sites can be broken down to 54 CCS from Santa Clara to Richardson, and 46 CCS from Richardson to Santa Clara, with the voice traffic 40 CCS (60 – 20) being the two-way traffic.
- The bandwidth requirement calculation would be:

$$(40/36) * 11.2 + (14/36) * 33.6 = 25.51 \text{ kbit/s}$$
 Where 14 CCS is the larger of two fax traffic parcels (14 CCS vs. 6 CCS).
- After adjusting for peaking, the incremental data rate on the WAN for this route is 33.2 kbit/s.
- Comparing this number with 24.3 kbit/s when all 60 CCS is voice traffic, it appears that the reduction in CCS due to one-way fax traffic (20 CCS vs. 14 CCS) will not compensate for the higher bandwidth requirement of a fax compared to a voice call (33.7 kbps vs. 11.2 kbps).

This section deals with nodal traffic calculation in both LAN and WAN. It indicates the incremental bandwidth requirement to handle voice on data networks.

At this point, enough information has been obtained to “load” the VoIP traffic on the intranet. Figure 23 on page 122 shows how this is done on an individual link.

Figure 23
Calculate network load with VoIP traffic



Suppose the intranet has a topology as shown in Figure 23 on page 122 and a prediction on the amount of traffic on a specific link, R4-R5, is required. From *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120) and Traceroute measurements, the R4-R5 link is expected to support the Santa Clara/Richardson, Santa Clara/Tokyo, and the Ottawa/Tokyo traffic flows; the other VoIP traffic flows do not route over R4-R5. The summation of the three flows yields 93 CCS or 24 kbit/s as the incremental traffic that R4-R5 will need to support.

As a final step, total the traffic flow for every site pair to calculate the load at each endpoint.

Route Link Traffic estimation

Routing information for all source-destination pairs must be recorded as part of the network assessment. This is done using the Traceroute tool. An example of the output is shown below.

```
Richardson3% traceroute santa_clara_itg4
traceroute to santa_clara_itg4 (10.3.2.7), 30 hops max, 32
byte packets
  r6 (10.8.0.1) 1 ms 1 ms 1 ms
  r5 (10.18.0.2) 42 ms 44 ms 38 ms
  r4 (10.28.0.3) 78 ms 70 ms 81 ms
  r1 (10.3.0.1) 92 ms 90 ms 101 ms
  santa_clara_itg4 (10.3.2.7) 94 ms 97 ms 95 ms
```

The Traceroute program is used to check if routing in the intranet is symmetric for each source-destination pair. Use the `-g` loose source routing option as shown in the following command example:

```
Richardson3% traceroute -g santa_clara_itg4 richardson3
```

A trace route command (rTraceRoute) is available at the Signaling Server Command Line Interface (CLI). This command traces a route from a remote IP Phone to another endpoint in the IP network.

The Traceroute tool identifies the intranet links that transmit VoIP traffic. For example, if Traceroute of four site pairs yield the results shown in Table 9, then the load of VoIP traffic per link can be computed as shown in Table 10 on page 124.

Table 9
Traceroute identification of intranet links (Part 1 of 2)

Site pair	Intranet route
Santa Clara/Richardson	R1-R4-R5-R6
Santa Clara/Ottawa	R1-R2

Table 9
Traceroute identification of intranet links (Part 2 of 2)

Site pair	Intranet route
Santa Clara/Tokyo	R1-R4-R5-R7
Richardson/Ottawa	R2-R3-R5-R6

Table 10
Route link traffic estimation

Links	Traffic from:
R1-R4	Santa Clara/Richardson +Santa Clara/Tokyo + Ottawa/Tokyo
R4-R5	Santa Clara/Richardson +Santa Clara/Tokyo + Ottawa/Tokyo
R5-R6	Santa Clara/Richardson +Richardson/Ottawa
R1-R2	Santa Clara/Ottawa + Tokyo/Ottawa
R5-R7	Santa Clara/Tokyo + Ottawa/Tokyo
R2-R3	Richardson/Ottawa
R3-R5	Richardson/Ottawa

Enough capacity

For each link, Table 11 on page 125 compares the available link capacity to the additional IP Trunk 3.0 (or later) load. For example, on link R4-R5, there is enough available capacity (492 kbit/s) to accommodate the additional 24 kbit/s of VoIP traffic.

Table 11
Computation of link capacity as compared to ITG load

Link		Utilization (%)		Available capacity (kbit/s)	Incremental IP Trunk 3.0 (or later) load		Sufficient capacity?
End-points	Capacity (kbit/s)	Threshold	Used		Site pair	Traffic (kbit/s)	
R1-R2	1536	80	75	76.8	Santa Clara/Ottawa + Ottawa/Tokyo	21.2	Yes
R1-R4	1536	80	50	460.8	Santa Clara/Tokyo + Santa Clara/Richardson + Ottawa / Tokyo	31.4	Yes
R4-R5	1536	80	48	492	Santa Clara/Richardson + Ottawa/Tokyo + Santa Clara/Tokyo	31.4	Yes

Some network management systems have network planning modules that compute network flows in the manner just described. These modules provide more detailed and accurate analysis, as they consider actual node, link, and routing information. They also help assess network resilience by conducting link and node failure analysis. By simulating failures and re-loading network and re-computed routes, the modules indicate where the network is out of capacity during failures.

Insufficient link capacity

If there is not enough link capacity, implement one or more of the following options:

- Use the G.723 CODEC series. Compared to the default G.729AB CODEC with 30 ms payload, the G.723 CODECs use 9% to 14% less bandwidth.
- Upgrade the link's bandwidth.

Other intranet resource considerations

Bottlenecks caused by non-WAN resources are less frequent. For a more complete assessment, consider the impact of incremental VoIP traffic on routers and LAN resources in the intranet. Perhaps the VoIP traffic is traversing LAN segments that are saturated, or traversing routers whose CPU utilization is high.

Delay

Delay is defined as the amount of time required for an application's data to reach its intended destination. Delay causes significant QoE issues with voice and video applications. Other applications, such as Fax transmissions, excessive delay causes the application to time-out and fail.

Some applications can compensate for specified amounts of delay, but once that amount is exceeded, QoS is compromised. VoIP and gateways also provide delay compensation by using local buffering.

Delay can be fixed or variable. Variable delay is also known as jitter.

Some contributions to fixed (baseline) delay are as follows:

- Application-based delay, such as:
 - voice CODEC processing
 - jitter buffer delay

- **Serialization delay** — Delay of the voice packet at each hop of the physical network; depends on link speed (a fixed, constant value for each link).
- **Propagation delay** — Delay caused by the finite speed at which electronic signals can travel through a transmission medium.

In VoIP, end-to-end delay on a call is the total time elapsed from speaking into an transmitter at one end to hearing the reconstructed sound on a receiver at the other end. Delay has a significant impact on the quality of a voice call. Most listeners can detect delay greater than 100 ms. Delay becomes annoying at the following levels:

- for G.711 CODEC, 250 ms
- for G.729AB CODEC, 150 ms

Figure 24 shows the sources of packet delay.

Figure 24
Sources of packet delay

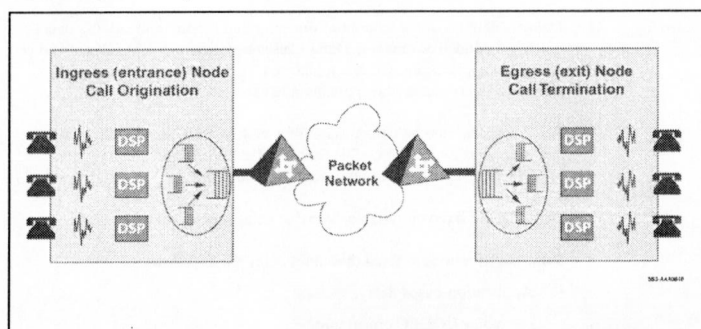


Table 12 lists the network elements where delay occurs, and the type of that delay.

Table 12
Delay characteristics of voice traffic

Packet action	Network element	Delay type
Entrance (ingress) node audio processing	Voice CODEC algorithmic processing	fixed delay
	Voice payload packetization	fixed delay
Entrance (ingress) node packet queueing	Packet contention for network port	variable delay
Data network transmission	LAN and WAN link speeds	fixed delay (per network segment type)
	Propagation over the network	fixed delay (per transmission distance)
	Packet contention at network nodes	variable delay
Exit (egress) node packet queueing	Packet contention for network port	variable delay
	Packet jitter buffer	fixed delay
Exit (egress) node audio processing	Voice decoder processing	fixed delay

Note: Table 12 does not account for enhanced applications, such as packet encryption, tunnelling, and Virtual Private Networks (VPNs), which adds delay due to the buffering of the extra payload, additional Digital Signal Processing (DSP), and from repacketization. These contributions to extra delay should be included in a delay analysis.

Effects of delay on voice quality

The overall "delay budget" for a voice call from the time one party speaks, to the time the voice is heard by the listener, should not exceed 150 ms for good quality voice over landline connections, although 250 ms is often tolerated for G.711 calls if there is no packet loss. (The amount of delay is often longer, but unavoidable, for satellite and other types of wireless connections).

Studies show that as the 150-ms delay budget is exceeded, users perceive the delay as resulting in poorer voice quality, especially for the compressed CODECs. Every time a VoIP packet passes through a device or network connection, delay is introduced. A significant amount of delay is introduced over low-bandwidth connections.

Components of delay

End-to-end delay is caused by many components. The major components of delay are as follows:

- Propagation delay
- Serialization delay
- Queuing delay
- Routing and hop count
- IP Trunk 3.0 (or later) system delay

Propagation delay

Propagation delay is affected by the mileage and medium of links traversed. Within an average-size country, one-way propagation delay over terrestrial lines is under 18 ms; within the U.S. the propagation delay from coast-to-coast is under 40 ms. To estimate the propagation delay of long-haul and trans-oceanic circuits use the rule-of-thumb of 1 ms per 100 terrestrial miles.

If a circuit goes through a satellite system, estimate each hop between earth stations to contribute 260 ms to the propagation delay.

Serialization delay

Serialization delay is the time it takes to transmit the voice packet one bit at a time over a WAN link. The serialization delay depends on the voice packet size and the link bandwidth, and is calculated using the following formula:

The following calculation is used to measure serialization delay in ms.

$$8 * (\text{IP packet size in bytes}) / (\text{link bandwidth in kbit/s})$$

Table 13 shows the serialization delay (in ms) for different packet sizes and link speeds.

Table 13
Serialization delay characteristics (in ms) for different packet sizes and link speeds

Link speed in Kbps	Packet size									
	40 bytes	80 bytes	88 bytes	136 bytes	184 bytes	232 bytes	280 bytes	520 bytes	1 Kbyte	1.48 Kbytes
56	5.7	11.4	12.5	19.4	26.	33.1	40.0	74.2	146.2	211.4
64	5.0	10.0	11.0	17.0	23.0	29.0	35.0	65.0	128.0	185.0
128	2.5	5.0	5.5	8.5	11.5	14.5	17.5	32.5	64.0	92.5
256	1.2	2.5	2.7	4.2	5.7	7.2	8.7	16.2	32.0	46.2
384	0.8	1.6	1.8	2.8	3.8	4.8	5.8	10.8	21.3	30.8
1000	0.3	0.6	0.7	1.0	1.4	1.8	2.2	4.1	8.1	11.8
1540	0.2	0.4	0.4	0.7	0.9	1.2	1.4	2.7	5.3	7.6
2048	0.1	0.3	0.5	0.71	0.9	1.09	2.0	4.0	4.0	5.7
10000	0.03	0.06	0.07	0.1	0.1	0.18	0.2	0.4	0.8	1.1
100000	0.003	0.006	0.007	0.01	0.015	0.019	0.022	0.04	0.08	0.1
150000	0.002	0.004	0.005	0.007	0.01	0.012	0.013	0.028	0.05	0.079

Table 14 shows the serialization delay for voice packets on a 64 kbit/s and 128 kbit/s link. The serialization delay on higher speed links are considered negligible.

Table 14
Serialization delay

CODEC	Frame duration	Serialization delay over 64 kbit/s link (ms)	Serialization delay over 128 kbit/s link (ms)
G.711A/ G.711U	10 ms	14.00	0.88
	20 ms	24.00	1.50
	30 ms	34.00	2.13
G.729A/ G.729AB	10 ms	5.25	0.33
	20 ms	6.50	0.41
	30 ms	7.75	0.48
G.723.1 5.3 kbit/s	30 ms	6.50	0.41
G.723.1 6.3 kbit/s	30 ms	7.00	0.44

Queuing delay

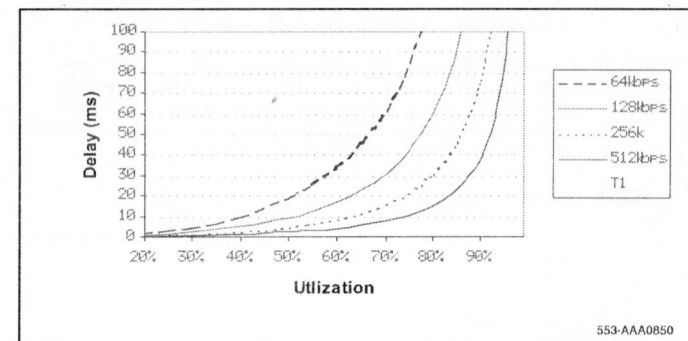
Queuing delay is the time it takes for a packet to wait in transmission queue of the link before it is serialized. On a link where packets are processed in first-come-first-serve order, the average queuing time in ms is estimated by the following formula:

$$p * p * (\text{average intranet packet in bytes}) / (1 - p) / (\text{link speed in kbit/s})$$

where p is the link utilization level.

The average size of intranet packets carried over WAN links generally is between 250 and 500 bytes. Figure 25 displays the average queuing delay of the network based on a 300-byte average packet size.

Figure 25
Queuing delay of various links



As can be seen in Figure 25 on page 132, queuing delays can be significant for links with bandwidth under 512 kbit/s. Higher speed links can tolerate much higher utilization levels.

Routing and hop count

Each site pair takes different routes over the intranet. The route taken determines the number and type of delay components that add to end-to-end delay. Sound routing in the network depends on correct network design at many levels, such as the architecture, topology, routing configuration, link and speed.

VoIP system delay

Together, the transmitting and receiving IP Trunk 3.0 (or later) nodes contribute a processing delay of about 33 ms to the end-to-end delay. This is the amount of time required for the encoder to analyze and packetize speech,

and is required by the decoder to reconstruct and de-packetize the voice packets.

There is a second component of delay that occurs on the receiving IP Trunk 3.0 (or later) node. For every call terminating on the receiver, there is a jitter buffer which serves as a holding queue for voice packets arriving at the destination ITG. The purpose of the jitter buffer is to smooth out the effects of delay variation, so that a steady stream of voice packets can be reproduced at the destination. The default jitter buffer delay for voice is 60 ms.

Other delay components

Other delay components, generally considered minor, are as follows:

- **Router (transit) processing delay**
The time it takes to forward a packet from one link to another on the router. In a healthy network, router processing delay is a few milliseconds.
- **LAN segment delay**
The transmission and processing delay of packets through a healthy LAN subnet is just one or two milliseconds.

Measuring end-to-end network delay

End-to-end delay and error characteristics of the intranet must be measured so the technician can set realistic voice quality expectations for intranet voice services.

The basic tool used in IP networks to measure end-to-end network delay is the PING program. PING takes a delay sample by sending an ICMP packet from the host of the PING program to a destination server, and waits for the packet to make a round trip.

Some implementations of PING support the `-v` option for setting the TOS. CS 1000 allows the 8-bit DiffServ/TOS field to be set to any value specified by the IP network administrator for QoS management purposes. For example, a decimal value of 36 entered in OTM 2.0 is interpreted as TOS Precedence = Priority and Reliability = High. If the `-v` option is not used, and if PING measurements are made on an intranet that uses prioritization based

on the TOS field, the round trip time (rtt) measured will be higher than the actual delay of voice packets. See "Queueing" on page 111.

Note: Ensure that the DiffServ bytes are set to their intended operational values before taking measurements.

CS 1000 also has a utility called rPing (remote ping) so an IP Phone can ping an IP address. The rPing command can be run from the Signaling Server OAM Command Line Interface (CLI). Refer to "Network Diagnostic Utilities" on page 229.

To ensure the delay sample results are representative of the IPLine_Node1 (see "Sample PING output:" on page 134):

- 1 Attach the PING host to a "healthy" LAN segment.
- 2 Attach the LAN segment to the router intended to support the IP Telephony node.
- 3 Choose a destination host by following the same critical guidelines as for the source host.

The size of the PING packets can be any number; the default is 60 bytes.

Sample PING output:

```
IPLine_Node1% PING -s subnetA 60
PING subnetA (10.3.2.7): 60 data bytes
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=100ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=102ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=95ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=94ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=112ms
68 bytes from (10.3.2.7): icmp_seq=0 ttl=225 time=97ms
^?
--- IPLine_Node1 PING Statistics ---
8 packets transmitted, 8 packets received, 0% packet
loss
round-trip (ms) min/avg/max = 94/96/112
```

Note: PING results can vary.

Assessment of sample PING output

Note: The round-trip time (rtt) is indicated by the time field.

The rtt from the PING output varies. It is from repeated sampling of rtt that a delay characteristic of the intranet can be obtained. To obtain a delay distribution, the PING tool can be embedded in a script that controls the frequency of the PING probes, timestamps and stores the samples in a raw data file. The file can then be analyzed later using a spreadsheet or another application. The technician can also check if the intranet's network management software has any delay measurement modules that can obtain a delay distribution for a specific route.

Delay characteristics vary depending on the site pair and the time-of-day. The site pair is defined as the measurement between the host IP Line and the remote subnet (for example, IP Line to subnet A in Figure 5 on page 33). The assessment of the intranet must include taking delay measurements for each IP Line site pair. If there is a significant variation of traffic on the intranet, include PING samples during the intranet's peak hour. For a complete assessment of the intranet's delay characteristics, obtain PING measurements over a period of at least one week.

Adjusting PING statistics

One-way and round-trip

PING statistics are based on round-trip measurements, while QoS metrics in the Transmission Rating model are one-way. Halve the delay and packet error PING statistics to ensure the comparison is valid.

Adjustment due to IP Line processing

PING statistics are measured from PING host to PING host. Transmission Rating QoS metrics are from end-user to end-user, and include components outside the intranet. The PING statistic for delay needs to be further modified by adding 93ms to account for the processing and jitter buffer delay of the nodes.

Note: There is no need to adjust error rates.

If the intranet measurement barely meets the round-trip QoS objectives, the technician must be aware of the possibility that one-way QoS is not being met in one of the directions of flow. This can apply even if the flow is on a symmetric route due to asymmetric behavior of data processing services.

Other measurement considerations

The PING statistics described above measure the intranet prior to CS 1000 installation, which means that the measurement does not take into consideration the expected load created by CS 1000 users.

If the intranet capacity is tight and the VoIP traffic significant, consider making intranet measurements under load. Load can be applied using traffic generator tools. The amount of load should match the IP Trunk-offered traffic estimated in the section "Estimate network loading caused by VoIP traffic" on page 118.

Reducing delays

Link delay is the time it takes for a voice packet to be queued on the transmission buffer of a link until it is received at the next hop router. Link delay can be reduced by:

- Upgrading link capacity — This reduces the serialization delay of the packet, but also reduces link utilization and queueing delay. Before upgrading a link, the technician must check both routers connected to the link to be upgraded and ensure compliance with router configuration guidelines.
- Implementing QoS mechanisms

To determine the links for upgrading, list all intranet links that support the IP Line traffic. This can be derived from the Traceroute output for each site pair. Use the intranet link utilization report and note the most used links and the slowest links. Estimate the link delay of suspect links using the Traceroute results.

Example

A 256 Kbps link from router1 to router2 has a high utilization. The following Traceroute output traverses this link:

```
IPLine_Node1% traceroute SubnetA
traceroute to SubnetA (10.3.2.7), 30 hops max, 32
byte packets
  router1 (10.8.0.1) 1 ms 1 ms 1 ms
  router2 (10.18.0.2) 42 ms 44 ms 38 ms
  router3 (10.28.0.3) 78 ms 70 ms 81 ms
  router4 (10.3.0.1) 92 ms 90 ms 101 ms
  SubnetA (10.3.2.7) 94 ms 97 ms 95 ms
```

The average rtt time on the example link is about 40 ms. The one-way link delay is about 20 ms, of which the circuit transmission and serialization delay are just a few milliseconds. Most of this link's delay is due to queueing.

Reducing hop count

Consider the current network topology and whether a more efficient design which reduces hop count can be implemented. Reducing hops reduces fixed and variable IP packet delay and improves VoIP QoS. It may also simplify end-to-end QoS engineering for packet delay, jitter, and packet loss.

Recording routes

The Traceroute tool records routing information for all source-destination pairs as part of the network assessment. An example of Traceroute output is shown below:

```
ipline_node1% traceroute subnetA
traceroute to subnetA 10.3.2.7, 30 hops max, 32 byte
packets
 1  r6 (10.8.0.1) 1 ms 1 ms 1 ms
 2  r5 (10.18.0.2) 42 ms 44 ms 38 ms
 3  r4 (10.28.0.3) 78 ms 70 ms 81 ms
 4  r1 (10.3.0.1) 92 ms 90 ms 101 ms
 5  subnetA (10.3.2.7) 94 ms 97 ms 95 ms
```

Traceroute is also used to verify whether routing in the intranet is symmetric for each source-destination pair. This is done using the -g loose source routing option, for example:

```
ipline_node1% traceroute -g subnetA ipline_node1
```

For information on the rTraceRoute command, refer to "Network Diagnostic Utilities" on page 229.

Routing issues

Unnecessary delay can be introduced by routing irregularities. A routing implementation might overlook a substantially better route. A high-delay variation can be caused by routing instability, incorrectly configured routing, inappropriate load splitting, or frequent changes to the intranet. Severe asymmetrical routing results in one site perceiving a poorer QoS than another.

The Traceroute program can be used to uncover these routing anomalies. Then routing implementation and policies can be audited and corrected.

Jitter

Jitter (also known as variable delay) is the variation in the amount of time it takes for consecutive packets to travel from sender to receiver. There is a fixed baseline delay (the absolute fastest time for a voice packet to pass through the network), and a variation in packet flow. The variation in the delay is jitter.

The primary cause of jitter (variable delay) is contention (competition for network access), also known as queueing delay. Variable delays are affected by the amount of network traffic.

Jitter has a pronounced effect on real-time, delay-sensitive applications, such as video and voice. These applications need to receive packets at a constant rate, with a fixed delay between consecutive packets. If the arrival rate varies, jitter occurs, and application performance degrades. Minimal jitter might be acceptable, but if jitter increases, the application could become unusable.

Some settings on devices such as VoIP gateways and IP Phones can compensate for a finite (specified) amount of jitter.

If an adaptive jitter buffer is used, delay is kept to a minimum during periods of low jitter. The adaptive buffer can adjust to higher levels of jitter, within a limited range, during periods of higher traffic volume. If the network becomes congested, jitter and packet loss can become undefined, and real-time interactive applications can become unusable.

Voice applications require the voice packets to be fed to the decoder at a constant rate. If the next voice packet does not arrive in time to take its turn to be decoded, the packet is considered lost. Packet Loss Concealment (PLC) attempts to smooth over the lost voice packet. PLC replays the previous voice packet until the next voice packet arrives. A PLC algorithm can repair losses of 40-60 ms. Longer gaps in the signal must be muted. If jitter is high, whole groups of packets can be late or lost, and output can contain muted segments.

All networks have some jitter. This is due to differences in delay at each network node, as packets are queued. If jitter is contained within specified limits, QoS can be maintained.

In VoIP, jitter is the total amount of variable delay encountered during the end-to-end processing of voice packets.

Jitter buffers are used on the receive-side of a call to smooth out small variations in the packet time-of arrival. This allows data to be unpacked and sent to the decoder as a constant stream. Since all buffering increases end-to-end delay, jitter buffer length (duration) must be kept to a minimum. If a network has been engineered to have minimal jitter, the jitter buffer can be very small.

The following factors contribute to the total variation in delay:

- packet contention during node queuing
- network conditions such as routing and transmission queuing
- router and switch (statistical multiplexer) performance under load
- link speed
- voice and data packet size
- exit (egress) queue buffer size

Queueing delay occurs at the exit port of every device on the network.

Call Admission Control (CAC) performs packet admission and blocking functions. Voice packets are admitted to the network when the network can adequately support them. The packets are denied admission when the network cannot support them as defined in the Service Level Agreement.

When voice and data packets share a low-speed WAN connection (< 1 Mbps), the larger data packets introduce queuing delay to the smaller voice packets waiting to be queued onto the WAN connection. Therefore, the smaller voice packets do not arrive at the same fixed time interval as they are transmitted from their source. The arrival time of the voice packets varies because interjected data packets of varying sizes introduce a varying amount of jitter (queuing delay).

Jitter buffers

When voice and data packets share a high-speed connection (> 1 Mbps), the jitter introduced by the WAN connection becomes insignificant. The jitter in high-speed networks is affected by the buffer size of a router and the load/congestion in the router. Jitter buffers are designed to smooth out irregular packet arrival. This is done by collecting incoming packets and holding them in a buffer long enough to allow the slowest packets to arrive. The packets are then played in the correct sequence. Jitter buffers solve the late and lost packet problem, but add to total end-to-end delay.

Late packets

Packets that arrive outside the window allowed by the jitter buffer are discarded by IP Line. To determine which PING samples to ignore, calculate the average one-way delay based on all the samples.

To calculate late packets, double the value of the nominal jitter buffer setting. For example, assume:

- the average one-way delay is 50 ms
- the jitter buffer is set to a nominal (or average) value of 40 ms
- then the maximum value is $2 \times 40 + 50 = 130$ ms

Therefore, any packet with a one-way delay of greater than 130 ms is late, and must be added to the total number of packets lost.

Adjusting jitter buffer size

The jitter buffer parameters directly affect end-to-end delay. Lowering the voice playout settings decreases one-way delay, but there is less waiting time for voice packets that arrive late.

The jitter buffer setting is configured on the voice gateway channels of the Voice Gateway Media Card, and are sent out to IP Phones. The jitter buffer size is set when configuring the DSP Profiles:

- in the IP Telephony application
- in the selected CODEC in Element Manager

The jitter buffer is statically configured and is the same for all devices in the network. The jitter buffer size range is 0-200 ms. The default jitter buffer value is 50 ms. However, the jitter buffer setting that is used on the Voice Gateway Media Card is a multiple of the CODEC frame size. The setting is automatically adjusted to be greater than or equal to the jitter buffer value set in the DSP Profile tab. As each call is set up, the jitter buffer for each device is set to the nearest whole number increment of the selected CODEC frame size.

For example, if the jitter buffer is configured as the default 50 ms in the DSP Profiles, but a 20 ms CODEC is used, the jitter buffer is set to 60 ms, which is the nearest whole number increment.

$$\begin{aligned} 50 \text{ ms} / 20 \text{ ms} &= 2.5 \\ 2.5 \text{ rounded up to the nearest whole number increment is } 3 \\ 3 \times 20 \text{ ms} &= 60 \text{ ms} \end{aligned}$$

If the jitter buffer is configured as zero, the depth of the jitter buffer is set to the smallest value the device can support. In practice, the optimum depth of the jitter queue is different for each call. For telephones on a local LAN connection, a short jitter queue is desirable to minimize delay. For telephones several router hops away, a longer jitter queue is required.

Lowering the jitter buffer size decreases the one-way delay of voice packets. If the setting for the jitter buffer size is too small, packets are discarded unnecessarily. Discarded packets result in poorer speech quality and can be heard as clicks or choppy speech.

If the technician decides to discard packets to downsize the jitter buffer, the technician must do the following:

- Check the delay variation statistics.
Obtain the one-way delay distributions originating from all source IP Line sites.
- Compute the standard deviation of one-way delay for every flow.
Some traffic sources with few hop counts yield small delay variations, but it is the flows that produce great delay variations that should be used to determine whether it is acceptable to resize the jitter buffer.
- Compute the standard deviation (S) of one-way delay for that flow.
Do not set the jitter buffer size smaller than 2 sec.

The IP Phone firmware must also be configured for jitter buffers. However, instead of specifying the jitter buffer size in ms, it is configured with the number of frames to be held in the jitter buffer, such as 1, 2, or 3.

Recommendation

To achieve maximum voice quality, Nortel strongly recommends that IP Phone firmware be configured with a jitter buffer size of 3; however, a well-engineered network can function with a jitter buffer size of 2, which increases perceived voice quality.

Jitter measurement tools

Once a CS 1000 system has been installed, the average jitter experienced by IP Phones or media cards may be monitored on a per-call basis by using the RTPTraceShow command from the signaling server CLI. The CS 1000 system can also be configured to transmit SNMP alarms if a certain average jitter level is exceeded. For more information, refer to "Proactive Voice Quality Management" on page 241.

Packet loss

Packet loss is the number of packets lost during transmission. It is usually measured as a percentage of the total packets exchanged.

Physical medium loss

Loss can occur due to errors created by the physical medium used to transmit the data.

Most landline connections have very low loss, measured in Bit Error Rate (BER). Wireless connections, such as satellite, mobile, or fixed wireless networks, have a high BER. The BER can vary due to the following:

- radio frequency interference
- cell hand-off during roaming calls
- weather conditions, such as fog and rain
- physical obstacles, such as trees, buildings, and mountains

Wireless technology usually transmits redundant information, since packets are often dropped during transmission due to the physical medium.

Congestion loss

Congestion loss consists of true loss (buffer overflow at router queues) and late packets. Loss also occurs when congested network nodes drop packets. The majority of packet loss is caused by congestion.

VoIP uses User Datagram Protocol (UDP). UDP is a connectionless protocol which, unlike TCP, cannot retransmit lost packets. A packet is sent from the source to the destination with no means to determine if that packet was received or not.

If a network becomes congested to the point that packets are lost, voice quality is degraded. Traffic is discarded if the transmit queue of an uplink has less bandwidth available than the total amount of bandwidth trying to use that link. This situation is also known as a "bottleneck".

Congestion can lead to packet loss. Mechanisms to avoid network congestion can be used. One such mechanism is called Random Early Discard (RED). RED deliberately drops packets once the network traffic reaches a specified threshold. The dropped packets cause TCP to reduce its window size and send fewer packets, thus reducing network traffic.

Note: RED provides congestion control only for applications or protocols that have the TCP-like ability to reduce network traffic.

UDP packets dropped in a network cannot be re-transmitted. Flow rates are not adjusted by devices that communicate through UDP.

Without discard priorities, it would be necessary to separate packets into different queues in a network node to provide different levels of service. This is expensive to implement, as only a limited number of hardware queues (usually eight or fewer) are available on networking devices. Though some devices have software-based queues, their increased use reduces network node performance.

With discard priorities, although packets are placed in the same queue, they are divided into virtual sub-queues, determined by their assigned discard priority. For example, if a product supports three discard priorities, then the product's queue provides three sub-queues, and therefore, three QoS levels.

Packets are usually lost due to a router dropping packets when links are congested.

Individual packets that are delayed much more than the baseline delay (variable delay) are referred to as jitter. Excess jitter causes packet loss which can result in choppy or unintelligible speech.

Packet loss occurs in the following situations:

- during network congestion
- misconfigured LAN settings
- misconfigured clock settings
- bit errors in the network

Recommendation

To achieve maximum voice quality, Nortel strongly recommends that packet loss = 0%.

Packet Loss Concealment (PLC) is used to minimize the noticeable effects of packet loss.

Measuring end-to-end packet loss

After a CS 1000 installation, use RTPTraceShow and PVQM SNMP alarms.

The PING program also reports whether the ICMP packet successfully completed its round trip. Use the same PING host setup to measure end-to-end error, and in making delay measurement, use the same packet size parameter.

Multiple PING samples must be used when sampling for error rate. Packet loss rate (PLR) is the error rate statistic collected by multiple PING samples. To be statistically significant, at least 300 samples must be used. Obtaining an error distribution requires running PING over a greater period of time.

For more information, refer to "Network Diagnostic Utilities" on page 229.

Packet Loss Concealment

The term **CODEC** stands for coder/decoder. A CODEC executes a compression algorithm (a specialized computer program) that reduces the number of bytes required to encode digital data. This reduces packet size and bandwidth requirements. As well, smaller packets are less likely to be lost.

CODECs designed for packet networks, such as G.729, have built-in Packet Loss Concealment (PLC). PLC minimizes the impact of lost packets on an audio signal, by mixing in synthesized speech derived from previous packets.

When a speech CODEC operates in normal mode, a receiver decodes packets and sends the output to an audio port. A PLC algorithm saves a copy of the recent audio output, which is used to create a signal to replace the missing speech if lost data is encountered. How this information is used depends on

the PLC algorithm. Some simple algorithms smooth over gaps in the signal to remove clicks. Other algorithms replay an earlier packet to fill in the gap. More sophisticated algorithms tweak the replacement signal to make it sound more natural. The best algorithms can repair a 20-40 ms gap with little audible distortion. The PLC operates constantly, generating speech to replace the next packet in the event it is lost. The use of a PLC adds a small fixed delay to the call's baseline delay.

PLC is necessary to achieve acceptable IP speech quality.

Reducing packet loss

Packet loss in intranets is generally related to congestion in the network. Bottlenecks in links are where the packet loss is high because packets get dropped, as the packets arrive faster than the link can transmit them. The task of upgrading highly utilized links can remove the source of packet loss on a particular flow. An effort to reduce hop count gives fewer opportunities for routers and links to drop packets.

Other causes of packet loss not related to queueing delay are as follows:

- **Poor link quality** — The underlying circuit could have transmission problems, high line error rates, and be subject to frequent outages. The circuit might possibly be provisioned on top of other services, such as X.25, Frame Relay, or ATM. Check with the service provider for information.
- **Overloaded CPU** — This is a commonly-monitored statistic collected by network management systems. If a router is overloaded, it means that the router is constantly performing processing-intensive tasks, which impede the router from forwarding packets. Determine the CPU utilization threshold and check if any suspect router conforms to it. The router may need to be re-configured or upgraded.
- **Saturation** — Routers can be overworked when configured with too many high capacity links and too many high traffic links. Ensure that routers are dimensioned according to vendor guidelines.
- **LAN saturation** — Packets may be dropped on under-engineered or faulty LAN segments.

- Jitter buffer too small — Packets that arrive at the destination, but too late to be placed in the jitter buffer, should be considered lost packets.
- Frame slips — Ensure that clocks are synchronized correctly.

Network delay and packet loss evaluation example

From PING data, calculate the average one-way delay (halved from PING output and adding 93 ms IP Trunk 3.0 (or later) processing delay) and standard deviation for latency. Do a similar calculation for packet loss without adjustment.

Adding a standard deviation to the mean of both delay and loss is for planning purposes. A customer might want to know whether traffic fluctuation in their intranet reduces the user's QoS.

Table 15 provides a sample measurement of network delay and packet loss for the G.729A CODEC between various nodes.

Table 15
Sample measurement results for G.729A CODEC

Destination pair	Measured one-way delay (ms)		Measured packet loss (%)		Expected QoS level (See page 151)	
	Mean	Mean+s	Mean	Mean+s	Mean	Mean+s
Santa Clara/Richardson	171	179	1.5	2.1	Excellent	Good
Santa Clara/Ottawa	120	132	1.3	1.6	Excellent	Excellent
Santa Clara/Tokyo	190	210	2.1	2.3	Good	Good
Richardson/Ottawa	220	235	2.4	2.7	Good	Good

As an example, the delay and loss pair of traffic from Santa Clara to Richardson (171 ms and 1.5%) will meet the "excellent" criterion, but their counterpart with standard deviation (179 ms and 2.1%) can achieve only "good" QoS.

In contrast, the site pair Santa Clara/Ottawa has both QoS levels of mean and mean+s falling in the excellent region. The customer has more confidence that during peak traffic period, the "excellent" service level is likely to be upheld (better than 84% chance under the assumption of Normal distribution).

Estimate voice quality

The perceived quality of a telephone call depends on many factors, such as CODEC characteristics, end-to-end delay, packet loss, and the perception of the individual listener.

The E-Model Transmission Planning Tool produces a quantifiable measure of voice quality based on relevant factors. Refer to two ITU-T recommendations (ITU-T E.107 and E.108) for more information on the E-Model and its application.

A simplified version of the E-Model is applied to provide an estimate of the voice quality that the user can expect, based on various configuration choices and network performance metrics.

The simplified E-Model is as follows:

$$R = 94 - I_c - I_d - I_p$$

where:

I_c = (see Table 16 on page 149)

I_d = delay impairment (see Table 17 on page 149)

I_p = packet loss impairment (see Table 18 on page 150)

Note: This model already takes into account some characteristics of the IP Phone, and therefore the impairment factors are not identical to those shown in the ITU-T standards.

See Table 19 for the translation of R values into user satisfaction levels.

Table 16
Impairment factors of CODECs

CODEC	CODEC Impairment (Ic) (ms frames)
G.711	0
G.711 a-law	8
G.711 mu-law	0
G.723.1	4
G.729A	18
G.729AB	
G.729A/AB	11 - 20 or 30
G.729A/AB	16 - 40 or 50
G.723.1 (5.3 Kbps)	19
G.723.1 (6.3 Kbps)	15

Table 17
Impairment factors due to network delay

Network delay* (ms)	Delay Impairment (Id)
0 - 49	0
50 - 99	5
100 - 149	10
150 - 199	15
200 - 249	20
250 - 299	25
* Network delay is the average one-way network delay plus packetization and jitter buffer delay.	

Table 18
Impairment factors due to packet loss

Packet loss (%)	Packet Lose Impairment (Ip)
0	0
1	4
2	8
4	15
8	25

Table 19
R value translation

R Value (lower limit)	MOS	User Satisfaction
90	4.5	Very satisfied
80	4.0	Satisfied
70	3.5	Some users dissatisfied
60	3.0	Many users dissatisfied
50	2.5	Nearly all users dissatisfied
0	1	Not recommended

Use Table 20 on page 151 to estimate the voice quality level based on performance measurements of the intranet. To limit the size of this table, the packet loss and one-way delay values are tabulated in increments of 1% and 10ms, respectively. The techniques used to determine and apply the information in this table are Nortel-proprietary.

Table 20
QoS levels (Part 1 of 2)

Network delay (ms)	Packet loss (%)	Voice quality level		
		G.711 20	G.729A/AB 30	G.723.1 (6.3 Kbps) 30
0 – 49	0	excellent	good	fair
	1	excellent	fair	fair
	2	good	fair	fair
	4	fair	poor	poor
	8	poor	not recommended	not recommended
50 – 99	0	excellent	fair	fair
	1	good	fair	fair
	2	good	fair	poor
	4	fair	poor	poor
99	8	poor	not recommended	not recommended
100 – 149	0	good	fair	fair
	1	good	fair	poor
	2	fair	poor	poor
	4	fair	poor	not recommended
	8	poor	not recommended	not recommended
150 – 199	0	fair	poor	poor
	1	fair	poor	good
	2	fair	poor	fair
	4	poor	not recommended	not recommended

Note: The QoS levels are equivalent to the following MOS values: excellent = 4.5, good = 4, fair = 3, poor = 2, and not recommended = less than 2.

Table 20
QoS levels (Part 2 of 2)

Network delay (ms)	Packet loss (%)	Voice quality level		
		G.711 20	G.729A/AB 30	G.723.1 (6.3 Kbps) 30
199	8	not recommended	not recommended	not recommended
200 – 249	0	poor	not recommended	not recommended
	1	poor	not recommended	not recommended
	2	poor	not recommended	not recommended
	4	not recommended	not recommended	not recommended
	8	not recommended	not recommended	not recommended
250 – 299	0	poor	not recommended	not recommended
	1	poor	not recommended	not recommended
	2	poor	not recommended	not recommended
	4	not recommended	not recommended	not recommended
	8	not recommended	not recommended	not recommended

Note: The QoS levels are equivalent to the following MOS values: excellent = 4.5, good = 4, fair = 3, poor = 2, and not recommended = less than 2.

Sample scenarios

Scenario 1

A local LAN has the following characteristics:

- G.711 CODEC
- 20 ms network delay
- 0.5% packet loss

To calculate $R = 94 - lc - ld - lp$, use Table 16 on page 149, Table 17 on page 149, and Table 18 on page 150:

- G.711 CODEC: $lc = 0$
- 20 ms network delay: $ld = 0$
- 0.5% packet loss: $lp = 2$

Then:

$$R = 94 - 0 - 0 - 2$$

$$R = 92$$

Using Table 20 on page 151, a value of 92 means the users are very satisfied.

Scenario 2

A campus network has the following characteristics:

- G.711 CODEC
- 50 ms delay
- 1.0% packet loss

To calculate $R = 94 - lc - ld - lp$, use Table 16 on page 149, Table 17 on page 149, and Table 18 on page 150:

- G.711 CODEC: $lc = 0$
- 20 ms network delay: $ld = 5$
- 0.5% packet loss: $lp = 4$

Then:

$$R = 94 - 0 - 5 - 4$$

$$R = 85$$

Using Table 20 on page 151, a value of 85 means that the users are satisfied.

Scenario 3

A WAN has the following characteristics:

- G.729 CODEC
- 30 ms network delay
- 2% packet loss

To calculate $R = 94 - lc - ld - lp$, use Table 16 on page 149, Table 17 on page 149, and Table 18 on page 150:

- G.711 CODEC: $lc = 11$
- 20 ms network delay: $ld = 5$
- 0.5% packet loss: $lp = 8$

Then:

$$R = 94 - 11 - 5 - 8$$

$$R = 70$$

Using Table 20 on page 151, a value of 70 means some users are dissatisfied.

Does the intranet provide expected voice quality?

At the end of this measurement and analysis, there should be a good indication if the corporate intranet in its present state can deliver adequate voice and fax services. Looking at the "Expected QoS level" column in Table 15 on page 147, the QoS level for each site pair can be gauged.

In order to offer voice and fax services over the intranet, keep the network within "Good" or "Excellent" QoS level at the Mean+s operating region. Fax services should not be offered on routes that have only "Fair" or "Poor" QoS levels.

If the expected QoS levels on some or all routes fall short of "Good", evaluate the options and costs to upgrade the intranet. Estimate the reduction in one-way delay that must be achieved to raise the QoS level. Often this involves a link upgrade, a topology change, or an implementation of QoS in the network.

A decision can be made to keep costs down and accept a temporary "Fair" QoS level for a selected route. In that case, having made a calculated trade-off in quality, carefully monitor the QoS level, reset expectations with the end users and be receptive to user feedback.

Recommendation

Nortel strongly recommends a minimum R-value of 70.

Configuration of the DHCP server

Contents

This section contains information on the following topics:

Overview	157
IP Phones	158
Partial DHCP mode	158
Full DHCP mode	159
802.1Q configuration of IP Phones	159
Configuring the DHCP server to support full DHCP mode	159
IP Phone class identifier	160
Requested network configuration parameters	160
Format for IP Phone DHCP Class Identifier option	162
Format for IP Phone DHCP encapsulated Vendor Specific Option	163
Format for IP Phone DHCP site-specific option	168

Overview

This chapter provides general guidelines on how to configure a host with a Dynamic Host Configuration Protocol (DHCP) server to support Nortel IP Phones 200x and the IP Softphone 2050.

Note 1: If not familiar with DHCP, Nortel recommends reading Request for Comments (RFC) 2131 "Dynamic Host Configuration Protocol", RFC 1533 "DHCP Options and BOOTP Vendor Extensions", and the Help manual for the DHCP server on the host.

Note 2: For a general overview of DHCP server technology, refer to Appendix C on page 279.

IP Phones

IP Phones 200x and the IP Softphone 2050 are VoIP telephones that function as a telephone to the Meridian 1 and CS 1000 systems. The IP Phone encodes voice as binary data and packetizes the data for transmission over an IP network to the Voice Gateway Media Card or to another IP Phone.

The Nortel IP Phone can act as a DHCP client in one of two modes:

- partial DHCP mode
- full DHCP mode

All the configuration parameters for the IP Phone can be entered manually. Each IP Phone requires the network configuration parameters, Connect Server parameters, IP Telephony node ID, and Virtual TN. If there are a number of IP Phones to configure, manual configuration is time-consuming and prone to error. Using full or partial DHCP to automatically configure the IP Phones is more efficient and flexible. This ensures that current information is used.

Partial DHCP mode

When the IP Phone is configured to operate in partial DHCP mode, the DHCP server needs no special configuration to support IP Phones. The IP Phone receives the following network configuration parameters from the DHCP server:

- IP address configuration for the IP Phone
- subnet mask for the IP Phone IP address
- default gateway for the IP Phone LAN segment

Note: In partial DHCP mode the Connect Server parameters, node ID and Virtual TN must be entered manually.

Full DHCP mode

In full DHCP mode, the DHCP server requires special configuration. The IP Phone obtains network configuration parameters and Connect Server configuration parameters from specially-configured DHCP servers.

The following parameters are provided for the primary and secondary Connect Servers:

- Connect Server IP address — for IP Line 4.5, the Connect Server IP address is the IP Telephony node IP address.
- port number = 4100
- command value = 1; identifies the request to the Connect Server as originating from an IP Phone
- retry count = 10 (typically)

Note: The IP Telephony node ID and Virtual TN must always be configured manually even in full DHCP mode.

802.1Q configuration of IP Phones

802.1Q VLAN support is configured using the display interface of the IP Phones during the initial configuration procedure of the IP Phone.

For 802.1Q configuration procedures of the IP Phones, see *IP Phones: Description, Installation, and Operation* (553-3001-368).

Configuring the DHCP server to support full DHCP mode

The DHCP capability of the IP Phone enables the telephone to receive network configuration parameters and specific Connect Server parameters. This section describes the IP Phone's unique class identifier and requested network configuration and Connect Server parameters for automatic configuration.

IP Phone class identifier

The IP Phone is designed with a unique class identifier that the DHCP server can use to identify the telephone. All Nortel IP Phones use the same text string, Nortel-i2004-A. The ASCII string is sent inside the Class Identifier option of the IP Phone's DHCP messages.

The DHCP server also includes this string in its responses to the IP Phone DHCP client. This makes it possible to notify the IP Phone that the server is IP Phone-aware, and that it is safe to accept the server's offer. This string appears in the beginning of a list of specific Voice Gateway Media Card information that the IP Phone DHCP client requests.

When the DHCP server is configured to recognize the IP Phone as a special class, the DHCP server can treat the IP Phone differently than other DHCP clients. DHCP host configuration parameters can then be grouped by class to supply only information relevant to the IP Phone DHCP client, such as the Connect Server parameters. The administrator can also design the network according to the client's class, if necessary, making maintenance easier.

Depending on the capabilities and limitations of the DHCP server used and the design of the network, some of these advanced functions are not available.

Requested network configuration parameters

Using full DHCP mode, an IP Phone-aware DHCP server can automatically configure Nortel IP Phones by requesting a list of Connect Server configuration parameters. The IP Phone uses DHCP to request and receive the information.

IP Phones operating in partial DHCP mode can receive an IP address from any DHCP server. In full DHCP mode, the server must be configured to respond to the request for the vendor-specific encapsulated options.

Table 21 lists the network configuration parameters requested by the IP Phone in the Parameter Request List option (Option Code 55) in the DHCPDISCOVER and DHCPREQUEST messages. The DHCP OFFER and

the DHCPACK reply messages from the DHCP server must contain the options in Table 21.

Table 21
IP Phone network configuration parameters

Parameters requested by IP Phone (Option Code 55)	DHCP server response: Option Code
Subnet mask — the client IP subnet mask	1
Router/gateway(s) — the IP address of the client's default gateway (not required in DHCPPOFFER in IP Phone Firmware 1.25 and later for compatibility with Novell DHCP server)	3
Lease time — implementation varies according to DHCP server	51
Renewal time — implementation varies according to DHCP server	58
Rebinding interval — implementation varies according to DHCP server	59
IP Line site-specific or vendor-specific encapsulated/site options.	43, 128, 144, 157, 191, 251

The first five parameters in Table 21 are standard DHCP options and have pre-defined option codes. The last parameter is for Voice Gateway Media Card information, which does not have a standard DHCP option. The server administrator must define a vendor-encapsulated and/or site-specific option to transport this information to the IP Phone.

This non-standard information includes the unique string identifying the IP Phone and the Connect Server parameters for the primary and secondary servers. The IP Phone must receive the Connect Server parameters to connect to the IP Telephony node.

The administrator must use one of the site-specific or vendor-encapsulated option codes to implement the Voice Gateway Media Card information. This

user-defined option can then be sent as-is, or encapsulated in a Vendor Encapsulated option with Option Code 43. The method used depends on the DHCP server's capabilities and what options are already in use by other vendors.

The IP Phone rejects any DHCPPOFFER and DHCPACK messages that do not contain the following options:

- a router option — IP Phone requires a default gateway (router)
- a subnet mask option
- a vendor-specific option (see Note 1) or a site-specific option (see Note 2)

Note 1: The vendor-specific option code is 43. A Windows NT DHCP Server (up to SR4) supports only 16 octets of data for the vendor-specific option, which is insufficient to support the minimum length of the IP Phone-specific string. If using a Windows NT DHCP Server, select the Site Specific option to accommodate the IP Phone-specific string.

Note 2: The site-specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for site-specific use by the DHCP RFCs.

Format for IP Phone DHCP Class Identifier option

All Nortel IP Phones fill in the Class ID option of the DHCPDISCOVER and DHCPREQUEST messages with the null-terminated, ASCII-encoded string Nortel-i2004-A, where A identifies the version number of the information format of the IP Phone.

The Class Identifier Nortel-i2004-A must be unique in the DHCP server domain.

Format for IP Phone DHCP encapsulated Vendor Specific Option

The following definition describes the Nortel-specific, encapsulated Vendor Specific Option for IP Phones 200x and the IP Softphone 2050. This option must be encapsulated in a DHCP vendor-specific option (refer to RFC 1533) and returned by the DHCP server as part of each DHCPOFFER and DHCPACK message for the IP Phone to accept these messages as valid. The IP Phone extracts the relevant information from this option and uses it to configure the Connect Server IP address, the port number (4100), a command value (1), and the retry count for the primary and secondary Connect Servers.

Either this encapsulated Vendor Specific Option or a similarly encoded site-specific option must be sent. The DHCP server must be configured to send one or the other, but not both. The choice of using the vendor-specific or the site-specific option is provided to enable Windows NT DHCP servers to support the IP Phone. Windows NT servers do not properly implement the Vendor Specific Option, and as a result, Windows NT implementations must use the Site Specific version.

The format of the encapsulated Vendor Specific option is Type, Length, and Data, described in the following sections.

Type (1 octet):

There are five types:

- 0x80 (Site Specific option 128)
- 0x90 (Site Specific option 144)
- 0x9d (Site Specific option 157)
- 0xbf (Site Specific option 191)
- 0xfb (Site Specific option 251)

The choice of five types enables the IP Phone to work one or more values are already in use by a different vendor. Select one value for the Type byte.

Length (1 octet)

The Length value is variable. Count only the number of octets in the data field (see the next section "Data (variable number of octets)").

Data (variable number of octets)

The Data field contains an ASCII-encoded character string as follows:

Nortel-i20xx-A,iii,jjj.kkk.lli:ppppp,aaa,rrr;iii,jjj.kkk.lli:ppppp,aaa,rrr.

This string can be NULL-terminated, although the NULL is not required for parsing.

The parameters for the data field are described in Table 22 and in the notes following the table.

Table 22
Data field parameters

Parameter	Description
Nortel-i2004-A	Uniquely identifies that this is the Nortel option, and is a response from a server that can provide the correct configuration information to the IP Phones 200x and the IP Softphone 2050.
iii,jjj.kkk.lli:ppppp	Identifies IP address and port number for server (ASCII-encoded decimal)
aaa	Identifies action for server (ASCII encoded decimal, range 0 – 255)
rrr	Identifies retry count for server (ASCII encoded decimal, range 0 – 255)
comma (,)	ASCII " ," separates fields.
colon (:)	ASCII ":" separates the IP address of the bootstrap server node IP address from the Transport Layer port number.
semicolon (;)	ASCII ";" separates the Primary from Secondary bootstrap server information. The bootstrap server is the Active Leader of the IP Telephony node.
period (.)	ASCII "." signals end of structure.

- “aaa” and “rrr” are ASCII encoded decimal numbers with a range of 0 – 255. They identify the “Action Code” and “Retry Count”, respectively, for the associated TPS server. They are stored as one octet (0x00 – 0xFF) in the IP Phone. These fields must be no more than three digits long.
- Two Connect Servers and an optional external application server (XAS) can be specified in the DHCP string:
 - The first Connect Server is always considered primary.
 - The second Connect Server is always considered secondary.
 - An optional XAS can be appended to the Connect Servers.
- The string enables the configuration of information for two Connect Servers. One Connect Server exists for each IP node. In the typical system configuration of a single IP node, only the primary Connect Server is required. In this case, the primary Connect Server string must end with a period (.) instead of a semi-colon (;). For example:

Nortel-i2004-A,iii,jjj,kkk.iii:ppppp,aaa,rrr.

If the secondary Connect Server portion of the string is specified, then the string information is typically the same as the primary Connect Server information. For example:

Nortel-i2004-A,iii,jjj,kkk.iii:ppppp,aaa,rrr;iii,jjj,kkk.iii:ppppp,aaa,rrr.

When the ‘Enhanced Redundancy for IP Line Nodes’ feature is used, two different Connect Server strings can be configured, separated with a semi-colon (;). This enables the telephone to register to two different nodes. For more information about the Enhanced Redundancy for IP Line Nodes feature, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

- Action code values:
 - 0 — reserved
 - 1 — UNISlim Hello (currently this type is the only valid choice)
 - 2 – 254 — reserved
 - 255 — reserved

- **iii,jjj,kkk.iii** are ASCII-encoded decimal numbers representing the IP address of the server. They do not need to be three digits long because the . and : delimiters guarantee parsing. For example, '001', '01', and '1' would be parsed correctly and interpreted as value 0x01 internal to the IP Phone. These fields must be no longer than three digits.
- **ppppp** is the port number in ASCII-encoded decimal. It does not need to be five digits long as the : and , delimiters guarantee parsing. For example, '05001', '5001', '1', '00001' would be parsed correctly and accepted as correct. The valid range is 0-65535 (stored internally in the IP Phone as hexadecimal in range 0 – 0xFFFF). This field must be no longer than five digits.
- In all cases, the ASCII-encoded numbers are treated as decimal values and all leading zeros are ignored. Specifically, a leading zero does not change the interpretation of the value to be OCTAL-encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.
- When using the Full DHCP option on the IP Phone 2004, the IP address of an XAS can be provided. To do this, append the XAS IP address and port to the Nortel DHCP option currently used to specify the first and second server IP address, ports, and retry and action codes.

The format of the exchange application server's IP address and port is:

iii,jjj,kkk.iii:ppppp

The port action code (aaa) and retry count (rrr) are not included.

Note: XAS always uses port 5000.

For example, the format of the option used to specify Connect Server 1, Connect Server 2, and the exchange application server (XAS) is:

Nortel-i20xx-A,iii,jjj,kkk.iii:ppppp,aaa,rrr;iii,jjj,kkk.iii:ppppp,aaa,rrr;iii,jjj,kkk.iii:ppppp.

Refer to the next section “Configuration string examples” for additional examples.

Configuration string examples

Tables 23 to Table 26 on page 168 show configuration strings with one or more Connect Servers and exchange application servers. The following conventions are used:

- The Nortel Class Identifier is separated from the servers by a comma (,).

- The servers are separated by semi-colons (;).
- The IP address and port numbers are separated by a colon (:).
- The string is terminated with a period (.)

Table 23
Configuration string for one Connect Server

Nortel-i2004-A,iii.jjj.kkk.lli:ppppp,aaa,rrr.	
Nortel Class Identifier Field	Primary Connect Server
Nortel-i2004-A	iii.jjj.kkk.lli:ppppp,aaa,rrr

Table 24
Configuration string for two Connect Servers

Nortel-i2004-A,iii.jjj.kkk.lli:ppppp,aaa,rrr;iii.jjj.kkk.lli:pppp,aaa,rrr.		
Nortel Class Identifier Field	Primary Connect Server	Secondary Connect Server
Nortel-i2004-A	iii.jjj.kkk.lli:ppppp,aaa,rrr	iii.jjj.kkk.lli:ppppp,aaa,rrr

Table 25
Configuration string for one Connect Server and an XAS

Nortel-i2004-A,iii.jjj.kkk.lli:ppppp,aaa,rrr;iii.jjj.kkk.lli:ppppp,aaa,rrr;iii.jjj.kkk.lli:pppp.			
Nortel Class Identifier Field	Primary Connect Server	Placeholder Secondary Connect Server	XAS
Nortel-i2004-A	iii.jjj.kkk.lli:ppppp,aaa,rrr	iii.jjj.kkk.lli:ppppp,aaa,rrr	iii.jjj.kkk.lli:ppppp

Note: Three IP addresses must be specified when using just one Connect Server and XAS. If only two IP addresses are specified, the IP Phone assumes the second IP address is for the second Connect Server. The IP Phone does not recognize that it is for the XAS. Therefore, a placeholder IP address must be inserted for the second Connect Server in this situation. The placeholder IP address ensures that the XAS IP address appears as the third address in the string (where the IP Phone expects to find it). Nortel recommends simply repeating the IP address of the first Connect Server for the second Connect Server, to create the placeholder IP address.

Table 26
Configuration string for two Connect Servers and an XAS

Nortel-i2004-A,iii.jjj.kkk.lli:ppppp,aaa,rrr;iii.jjj.kkk.lli:ppppp,aaa,rrr;iii.jjj.kkk.lli:pppp.			
Nortel Class Identifier Field	Primary Connect Server	Secondary Connect Server	XAS
Nortel-i2004-A	iii.jjj.kkk.lli:ppppp,aaa,rrr	iii.jjj.kkk.lli:ppppp,aaa,rrr	iii.jjj.kkk.lli:ppppp

Format for IP Phone DHCP site-specific option

This section describes the Nortel-specific, site-specific option for the IP Phones 200x, and the IP Softphone 2050. This option uses the "reserved for site specific use" DHCP options (128 to 254) (refer to RFC 1541 and RFC 1533), and must be returned by the DHCP server as part of each DHCP OFFER and DHCP ACK message for the IP Phone to accept these messages as valid.

The IP Phone retrieves the relevant information and uses it to configure the IP address for the primary TPS and optional secondary TPS. Either this site-specific option must be present or a similarly encoded vendor-specific option must be sent. That is, configure the DHCP server to send one or the other but not both. The choice of using either vendor-specific or site-specific options enables Windows NT DHCP servers to be used with the IP Phone. Windows NT servers do not properly implement the vendor-specific option and as a result, Windows NT implementations must use the site-specific version.

The format of the option is Type, Length, and Data. The format of the same as that of the encapsulated vendor-specific option (see "Format for IP Phone DHCP encapsulated Vendor Specific Option" on page 163).

Server LAN design

Contents

This section contains information on the following topics:

Introduction	170
Server subnets	171
CS 1000 Ethernet connections	175
Ethernet requirements	181
General Layer 2 considerations	181
CS 1000 network interfaces	182
Broadcast and Multicast rate limiting	184
Network interface half- and full-duplex operation	185
Spanning Tree options on Layer 2 switches	186
How to avoid system interruption	186
IP address requirements	188
General requirements for node IP addressing	189
ELAN and TLAN subnet configuration examples	192
Selecting public or private IP addresses	194
ELAN and TLAN network interfaces on a single subnet	195
Multiple nodes on the same ELAN and TLAN subnets	196
Guidelines for configuring a routable ELAN subnet	197
Redundant LAN design	197
Single physical location	197
CS 1000E Campus redundancy	202
Distributed IP Expansion Media Gateway requirements	203
IP expansion link requirements	204

Bandwidth planning	205
Monitoring IP expansion link QoS	206
IP expansion link Packet Delay Variation jitter buffer	207
Distributed Media Gateway 1000E	208
Campus-distributed Media Gateway enhancements	209
Campus-distributed Media Gateway 1000E IP address configuration	210
Sample system layout	211
Address and connection tables	211

Introduction

This chapter describes the requirements for creating and maintaining a robust, redundant server network.

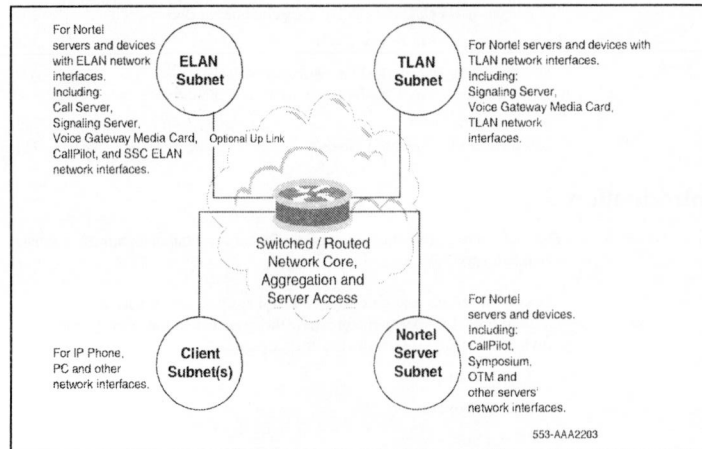
The system servers and gateways can require up to four separate sub-networks. In order to differentiate the subnets and the corresponding network interface on each device, they are named:

- ELAN subnet
- TLAN subnet
- Nortel Server subnet

The fourth subnet, although not requiring any Layer 2 or Layer 3 switches, is for the IP expansion links network interfaces which connect SSC cards in a CS 1000S or Media Gateway 1000T (MG 1000T).

Figure 26 on page 171 shows the logical elements of basic system connectivity in a CS 1000 network.

Figure 26
Example: Enterprise IP Network (that is, describing the whole of the data network structure)

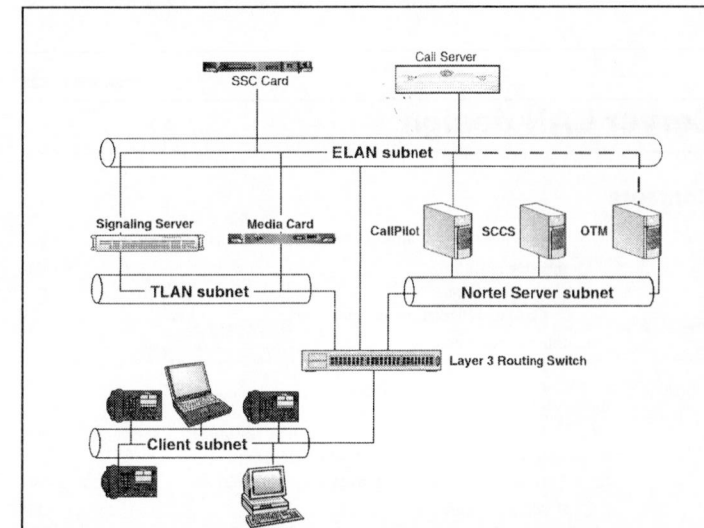


Note: Every device, with the exception of the Call Server, has an ELAN and a TLAN network interface. VoIP Desktop Clients on a QoS-managed IP network are usually separate subnets from the ELAN, TLAN, and Nortel server subnets.

Server subnets

Figure 27 on page 172 shows the Ethernet connection model in a CS 1000 network.

Figure 27
Layer 2 Ethernet connection model



ELAN subnet

The ELAN subnet is an isolated 10BaseT subnet required for management traffic and intra-system signaling traffic between the system Call Server and any devices requiring Call Server processing (for example, the Signaling Server, SSC cards, Voice Gateway Media Cards, CallPilot, and Symposium).

The ELAN subnet must create an isolated broadcast domain. Use of a Virtual LAN or a physically separate Layer 2 switch is acceptable. This reduces the risk of network outage due to broadcast storms or other extraneous network traffic.

Only Nortel servers with an ELAN network interface can be connected to the ELAN subnet. Do not connect other PCs or clients to the ELAN subnet. For example, connect the ELAN network interface from other applications, such as CallPilot and Symposium Call Center Server, to the ELAN subnet.

Configure any Windows-based servers with an ELAN network interface, and a second network interface connected to another subnet (for example, SCCS, CallPilot, and OTM servers). Do not transmit extraneous traffic, such as broadcasts or multicasts, onto the ELAN subnet.

Nortel recommends a Layer 2 switch with broadcast and multicast rate limiting, for the ELAN subnet. A Layer 2 switch with broadcast and multicast rate limiting features improves the robustness of all servers. Implement rate limiting for an isolated ELAN subnet, even if the Layer 2 switch is not connected to the rest of the network.

For information on designing a CS 1000 server network for maximum redundancy, see "Redundant LAN design" on page 197.

The ELAN subnet also carries system management traffic. An uplink from the ELAN subnet to the enterprise IP network becomes necessary if using OTM or SNMP to manage a network of CS 1000 or Meridian 1 systems. If planning to connect the ELAN subnet to the enterprise IP network, a Layer 3 switch or router capable of packet filtering must be used to separate the ELAN subnet from the enterprise IP network. The Layer 3 switch must be configured to prevent random broadcast, multicast traffic from entering the ELAN subnet. The Layer 3 switch must also be configured with a packet filter to prevent unauthorized traffic from entering the ELAN subnet. If the ELAN subnet is connected to the enterprise IP network without a packet-filtering Layer 3 switch or router, the system's call-handling ability may be adversely affected.

In the case of a single CS 1000 system, the OTM server can be connected to the ELAN subnet, removing the need for the uplink from the ELAN subnet to the rest of the enterprise IP network. Refer to *Optivity Telephony Manager: Installation and Configuration* (553-3001-230) for information on connecting the OTM server to the IP network.

TLAN subnet

The TLAN subnet is a 100BaseT full-duplex LAN that connects all Voice Gateway Media Cards and Signaling Servers within an IP telephony node. An IP telephony node is defined as a logical grouping of Voice Gateway Media Cards and Signaling Servers.

A device in a single IP telephony node cannot be a member of more than one subnet/VLAN. However, a subnet can have more than one IP telephony node as a member.

Use of a Layer 2 switch with broadcast and multicast rate limiting is recommended for the TLAN subnet.

Recommendation

Nortel strongly recommends use of a Layer 2 switch with broadcast and multicast rate limiting for the TLAN subnet.

Nortel further recommends that customers configure the TLAN subnet to carry only CS 1000-specific traffic, and be separated from the rest of the enterprise IP network by a Layer 3 switch. Deploy the IP Phones on the client side of the enterprise IP network.

Optionally, the TLAN subnet can be configured as a restricted-access subnet. This can be implemented using a packet filtering device (for example, a firewall) to restrict traffic, based on source IP address or TCP/UDP port numbers, allowed to enter the TLAN subnet.

Nortel recommends that port prioritization for all TLAN connections. For detailed information on port prioritization, see "QoS mechanisms" on page 47.

Nortel Server subnet

The Nortel Server subnet is the least specialized of the four subnets described in this chapter. Nortel recommends that the Nortel Server subnet be used to connect the CLAN network interfaces on the CallPilot, Symposium, and OTM servers as well as any other Nortel servers or applications associated with these systems.

Recommendation

Nortel strongly recommends that the Nortel Server subnet be separated from the rest of the enterprise IP network by a Layer 3 switch.

Optionally, you can connect the CLAN network interfaces of the CallPilot, Symposium, and OTM server to the dedicated Nortel Server subnet, or to any non-dedicated subnet (for example, shared with other servers) in the customer's enterprise IP network.

Recommendation

Nortel strongly recommends the use of a Layer 2 switch for the Nortel server subnet.

The TLAN subnet and the Nortel Server subnet can be the same subnet.

CS 1000 Ethernet connections

Figure 28 on page 176 through Figure 33 on page 181 shows CS 1000 server and gateway network connectivity at Layer 1 and Layer 2.

These figures also show redundant Layer 2 switches utilizing virtual LANs to group the ELAN and TLAN subnets. Refer to "Redundant LAN design" on page 197 for more information on Layer 2 and Layer 3 switch redundancy. In all cases, a single Layer 2 switch (or a single Layer 2 switch designated for the ELAN and TLAN subnets) can be used, but at the cost of system reliability.

Figure 28
MG 1000B detailed core system connections

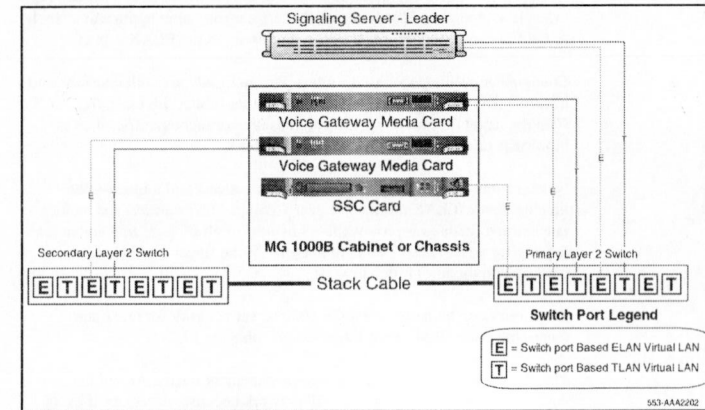


Figure 29
CS 1000E - Physically co-located Side 0 and Side 1

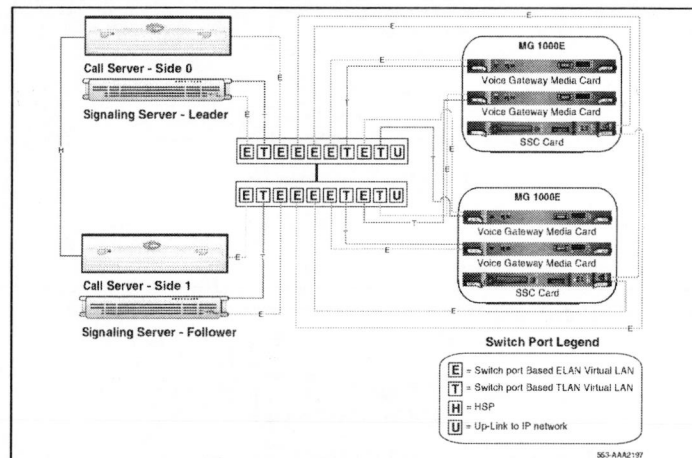
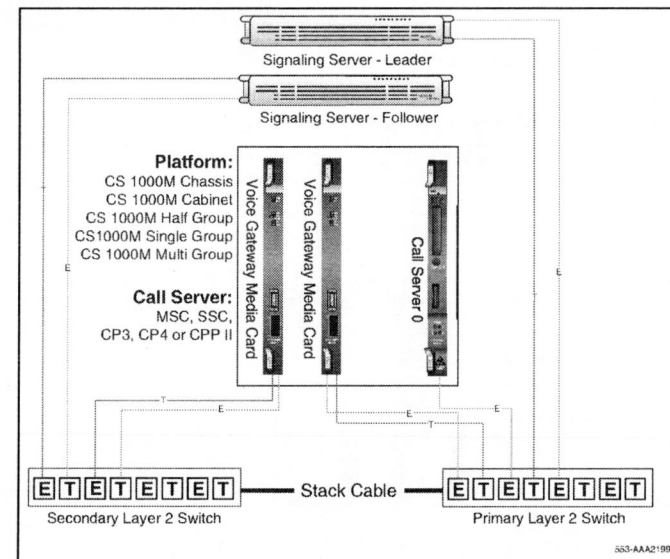


Figure 30
CS 1000M



Note 1: It is possible to connect the Call Server HSP through a Layer 2 switch providing specified network parameters are met.

Note 2: It is possible to separate the Call Server ELAN from the MG1000E using a Layer 3 switch/router providing network parameters are met.

Figure 30 is a generic diagram for the following platforms:

- CS 1000M Chassis

- CS 1000M Cabinet
- CS 1000M HG
- CS 1000M SG
- CS 1000M MG

Figure 31
CS 1000M MG with dual CP PII or CP PIV Call Server cards

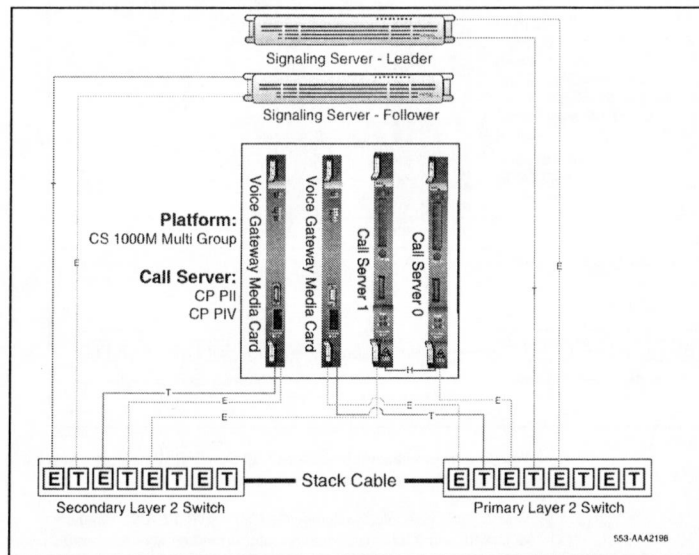


Figure 32
CS 1000S

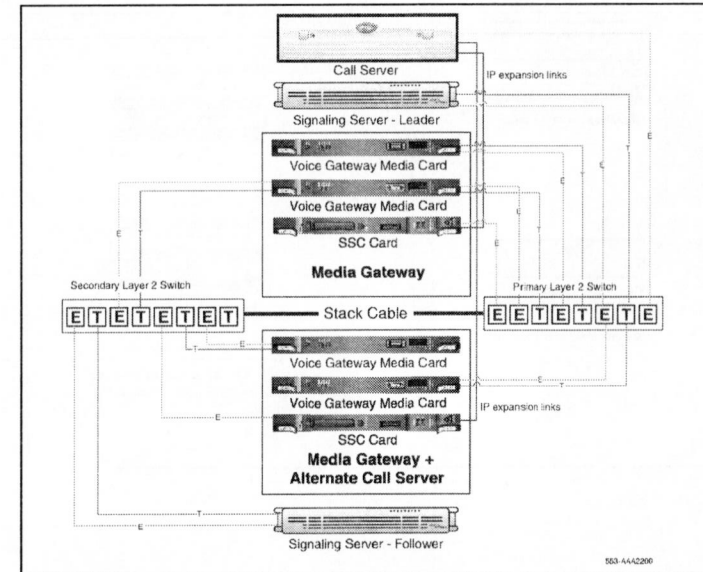
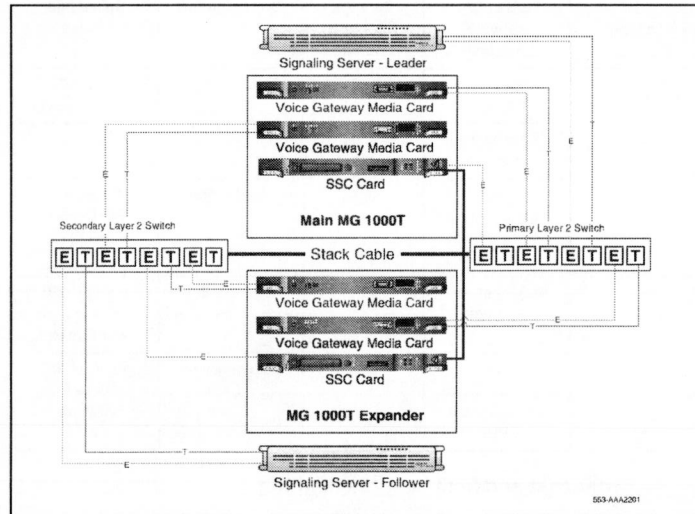


Figure 33
CS 1000T



Ethernet requirements

Careful consideration must be given to the Layer 2 infrastructure that the system is connected to. This section describes issues that must be considered when designing the server LAN connecting a system to the IP network.

General Layer 2 considerations

Passive Ethernet hubs are not supported. Use Layer 2 Ethernet switches for both the ELAN and TLAN subnets. Ideally, managed switches should be used.

The general requirements are as follows:

- no foreign broadcast coming from other subnets
- no BootP relay agent requirement (only on ELAN subnets router interface)
- the TLAN ethernet cable between the ITG-P Line Card and the Layer 2 switch must be 50 meters or less
- disable Spanning Tree protocol or enable "port fast" on the Layer 2 switch network interfaces connected to the ELAN and TLAN ports of the Meridian 1, CS 1000S, and CS 1000M components.

CS 1000 network interfaces

The devices in the system have different network interface names depending on whether the devices are on the TLAN or on the ELAN subnets. Table 27 on page 182 shows the network interface card names for the Voice Gateway Media Cards (Media Card 32-port card and ITG-P 24-port card), the Signaling Server, Small System Controller (SSC), and Call Processor Pentium (CPP).

Table 27
Network Interface Card Names (Part 1 of 3)

Device type	TLAN/ELAN network interface	Network interface name	Configuration	Speed and duplex
Media Card	ELAN network interface	ixpMac1	Auto-negotiate	10BaseT Half Duplex
	TLAN network interface	ixpMac0	Auto-negotiate	100BaseT Full Duplex
ITG-P Line Card	ELAN network interface	InIsa0	Auto-negotiate	10BaseT Half Duplex
	TLAN network interface	InPci1	Auto-negotiate	100BaseT Full Duplex

Table 27
Network Interface Card Names (Part 2 of 3)

Device type	TLAN/ELAN network interface	Network interface name	Configuration	Speed and duplex
Signaling Server	ELAN network interface	fei0	Auto-negotiate	100BaseT Full Duplex
	TLAN network interface	fei1	Auto-negotiate	100BaseT Full Duplex
SSC	ELAN network interface	qu0	Auto-negotiate	10BaseT Half Duplex
	TLAN network interface	not applicable		
	IPDB network interface 1	ipDB0	Auto-negotiate	100BaseT Full Duplex
	IPDB network interface 3	ipDB2	Auto-negotiate	100BaseT Full Duplex
	IPDB network interface 2	ipDB1	Auto-negotiate	100BaseT Full Duplex
	IPDB network interface 4	ipDB3	Auto-negotiate	100BaseT Full Duplex
CP3	ELAN network interface	ln0	Auto-negotiate	10Base T Half Duplex
CP4	ELAN network interface	ln0	Auto-negotiate	10BaseT Half Duplex

Table 27
Network Interface Card Names (Part 3 of 3)

Device type	TLAN/ELAN network interface	Network interface name	Configuration	Speed and duplex
CP PII	ELAN network interface	fei0	Auto negotiate	100BaseT Full Duplex
	TLAN network interface	not applicable		
	HSP (high-speed pipe for redundant CPUs)	fei1	Hard coded	100BaseT Full Duplex
CP PIV	ELAN network interface	gei0	Auto negotiate	10/100/1000 BaseT Full Duplex
	HSP (high-speed pipe for redundant CPUs)	gei1	Auto negotiate	10/100/1000 BaseT Full Duplex

Broadcast and Multicast rate limiting

Rate limit all broadcast traffic in the ELAN and TLAN Layer 2 or Layer 3 switch to 150 broadcast packets per second (pps). Rate limit all multicast traffic in the ELAN and TLAN Layer 2 or Layer 3 switch to 150 broadcast pps. In some Layer 2 and Layer 3 switches it may be possible, and is recommended, to disable transmission of multicast packets entirely.

Apply the broadcast and multicast rate limiting at egress from the switch ports, or optionally configure all switch ports to rate limit ingress broadcast and multicast traffic. Rate limiting is in addition to the guidelines in "Guidelines for configuring a routable ELAN subnet" on page 197.

Network interface half- and full-duplex operation

The ELAN network interface on the Voice Gateway Media Card operates at half-duplex only and is limited to 10BaseT operation due to filtering on the CS 1000M Cabinet and CS 1000M Chassis back planes.

The TLAN network interface on Voice Gateway Media Card operates at half-duplex or full-duplex and can run at 10BaseT or 100BaseT.

Nortel recommends that any Layer 2 or Layer 3 switch ports connected to the ELAN or TLAN network interfaces be set to Auto-sense/Auto-negotiate for correct operation. Although full-duplex is preferred, it is not required. For example, for the IP Line application, half-duplex has ample bandwidth for a Voice Gateway Media Card with 24 busy channels, VAD disabled, and G.711 CODEC with 10 ms voice range.

Mismatches can occur if devices are hard configured for speed and duplex mode. Every device and port must be correctly configured to avoid duplex mismatch problems that are indicated by lost packets and CRC errors. The Voice Gateway Media Card cannot be hard-coded for 100BaseT/full-duplex operation, so the TLAN network interface operates in Auto Negotiate mode. Duplex mismatches and lost packets occur if the TLAN network interface is not configured properly.

**CAUTION**

Duplex mismatches occur in the LAN environment when one side is set to Auto-negotiate, and the other is hard-configured.

The Auto-negotiate side adapts only to the speed setting of the fixed side. For duplex operations, the Auto-negotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

Spanning Tree options on Layer 2 switches

Nortel recommends disabling the Spanning Tree option on the Layer 2 switch ports that connect to the TLAN and ELAN network interfaces on the Meridian 1, CS 1000S, and CS 1000M systems.

This option is enabled by default on most Layer 2 switches. If the option is left enabled, the subsequent Spanning Tree discovery algorithm initiated when a device connected to a port is reset, rebooted, or repowered, can interfere with the Master Election Process in the Meridian 1, CS 1000S and CS 1000M system devices. In most cases the Master Election Process recovers from this after a slight delay. However, Nortel recommends that the Spanning Tree option on these ports be disabled or the Port Fast option enabled.

How to avoid system interruption

Duplex mismatch

Duplex mismatches can occur in the LAN environment when one side is set to auto-negotiate and the other is hard-configured. The auto-negotiate side adapts to the fixed-side settings, including speed. For duplex operations, the auto-negotiate side sets itself to half-duplex mode. If the forced side is full-duplex, a duplex mismatch occurs.

To hard-configure all devices for speed/duplex, ensure every device and port is correctly configured in order to avoid duplex mismatch problems.

**WARNING**

Configure the Layer 2 or Layer 3 switch ports as **Auto-negotiate**.

If one side is manually configured and the other side is configured as Auto-negotiate, the following situation occurs:

The auto-negotiate side sets itself to the manually configured side's speed, but always sets itself to half-duplex. If the manually-configured side is full-duplex, then a duplex mismatch occurs and voice quality is unsatisfactory.

Recommendation

Nortel strongly recommends that all Layer 2 ELAN and TLAN switch ports be set to auto-negotiate.

I/O filter connector

The other major TLAN network interface operation problem arises from the standard I/O filter connector in IPE modules on Meridian 1 Large Systems and CS 1000M Large Systems.

Use the following guidelines to avoid system interruption stemming from the standard I/O filter connector in IPE modules:

- Ensure that the standard IPE module I/O filter is replaced with the provided Voice Gateway Media Card/ITG-specific filter connector that removes filtering from pairs 23 and 24.
- Do not install the Voice Gateway Media Card/ITG-specific filter connector on top of the standard IPE module I/O filter connector.
- Replace the IPE module backplane I/O ribbon cable assemblies with those that have interchangeable I/O filter connectors.
- The CAT-5 Ethernet cable from the TLAN network interface to the Layer 2 switch port must meet the UTP Category 5 termination and impedance uniformity standards.

- The CAT-5 Ethernet cable from the TLAN network interface of the ITG Pentium card to the Layer 2 switch port must not exceed 50 meters in length.

The TLAN network interface can auto-negotiate to 100BaseT full-duplex. For the TLAN network interface to operate correctly at 100 Base T full-duplex speeds, do the following:

- Install the Voice Gateway Media Card/ITG-specific filter connector correctly by replacing the standard IPE Module I/O filter connector.
- Order new IPE Module Backplane I/O ribbon cable assemblies that have interchangeable I/O filter connectors if it becomes necessary to use one of the IPE Modules with molded-on I/O filter connectors.
- Ensure that the UTP cabling is CAT-5 compliant.
- Always keep the CAT-5 Ethernet cable from the TLAN network interface to the Layer 2 switch port less than 50 meters for the ITG-Pentium 24-port trunk card.
- As an interim measure, connect to each ITG-Pentium 24-port trunk card and log in to the ITG> shell. In the shell, use the commands `tlanDuplexSet` and `tlanSpeedSet` to set the TLAN network interface to operate at half-duplex 10BaseT.

IP address requirements

This section describes IP address requirements for each node, card, and IP Phone.

A node is a group of ITG-P Line Cards and Media Cards in a given Meridian 1 or CS 1000 system. Each card in a node has two IP addresses: one for the TLAN network interface and one for the Meridian 1 or CS 1000 ELAN network interface. Each node has one Node IP address on the TLAN subnet that is dynamically assigned to the connection server on the node Master. The IP Phone uses the Node IP address during the registration process.

All CS 1000 ELAN network interface IP addresses must be on the same subnet as the system's Call Server ELAN network interface IP address.

General requirements for node IP addressing

The configure a node, the following IP addresses must be assigned:

- One IP address for each TLAN network interface of every Voice Gateway Media Card and Signaling Server.
- One IP address for each ELAN network interface of every Voice Gateway Media Card and Signaling Server.
- One TLAN Node IP address. This alias IP address appears dynamically on the TLAN network interface of one card in the node, the Leader or node Master. This address is shared among all the cards.
- On CS 1000 systems, one IP address for the Signaling Server ELAN network interface and Signaling Server TLAN network interface.

In addition to the IP addresses that must be assigned, the following network information must be provided:

- ELAN network interface subnet mask
- ELAN network interface default gateway IP address
- TLAN network interface subnet mask
- TLAN network interface default gateway IP address

Note: Use separate ELAN and TLAN subnets with the Voice Gateway Media card. The user interface provides an option to use the same subnets, but you must use different subnets.

The default setting of separate ELAN and TLAN subnets protects the subnet from extraneous network traffic, including broadcast and multicast storms. It may also protect the Call Server from unauthorized access from the customer's enterprise network.

Recommendation

Nortel strongly recommends using separate dedicated ELAN and TLAN virtual LANs and subnet. They must be separated by a router/Layer 3 switch.

If it is necessary to use a single ELAN and TLAN subnet, see "ELAN and TLAN network interfaces on a single subnet" on page 195.

Call Server IP address requirements

The Call Server IP address is the IP address of the Call Server on the ELAN subnet. The Call Server ELAN network interface's IP address must correspond to the Active ELNK IP address configured in LD 117. Specifically:

- one IP address for the Call Server's ELAN network interface
- two IP addresses for each daughterboard link on a CS 1000M Small System:
 - One IP address is on the Call Server.
 - The other IP address is on the MG 1000S Small System Controller.

The Alternate Call Server ELAN network interface IP address must be in the same ELAN subnet as the Primary Call Server ELAN network interface IP address

MG 1000E IP address requirements

The SSC card requires:

- one IP address on the ELAN subnet
- one IP address for the IP daughter network interface connected to the ELAN subnet

Signaling Server IP address requirements

The Signaling Server has a TLAN network interface and an ELAN network interface, as follows:

- one IP address for the Signaling Server's ELAN network interface
- one IP address for the Signaling Server's TLAN network interface

The IP addresses are configured in the Signaling Server Install Tool menu. Follower Signaling Servers are configured using CS 1000 Element Manager running on the Leader Signaling Server. For more information about the Signaling Server, refer to *Signaling Server: Installation and Configuration* (553-3001-212).

Network Routing Service IP address requirements

The Network Routing Server (NRS) software can be run on a Signaling Server in stand-alone mode with no other applications, or it can run in co-resident mode with other applications such as the Line TPS and Media Gateway 1000T (MG 1000T).

For a standalone NRS, only the TLAN network interface is required. A node IP address and a TLAN network interface IP address must be configured on the standalone NRS. Use of the ELAN network interface is not required. When asked to enter an ELAN IP address, assign a private IP address. For example, 10.10.0.1 with mask 255.255.255.0. Do not configure a Call Server IP address.

For a co-resident NRS, the Signaling Server IP address requirements apply:

- one IP address for the Signaling Server's ELAN network interface
- one IP address for the Signaling Server's TLAN network interface

The NRS IP address is the TLAN network interface IP address of the Signaling Server.

The ELAN and TLAN network interface IP addresses, and the NRS IP addresses, are configured from the Signaling Server Install Tool menu. Follower Signaling Servers are configured using Element Manager running on the Leader Signaling Server.

Voice Gateway Media Card IP address requirements

Provide an IP address for both the ELAN and TLAN network interfaces. All cards must be connected to the same ELAN subnet, which is also the same subnet to which the system's Call Server is connected. All cards in a node must be connected to the same TLAN subnet.

The ELAN network interface MAC address corresponds to the Management MAC address, which is assigned during manufacturing and cannot be changed. Locate the faceplate sticker on the Voice Gateway Media Card. The ELAN/Management MAC address is the MOTHERBOARD Ethernet address.

The Voice Gateway Media Card IP addresses are configured using Element Manager or OTM.

Use separate subnets for the IP Telephony node. Each Voice Gateway Media Card configuration requires the following:

- Management (ELAN network interface) IP address
- Voice (TLAN network interface) IP address
- Management MAC address
- Voice LAN gateway IP address

ELAN and TLAN subnet configuration examples

The following restrictions apply:

- The Leader 0 and Leader 1 cards must co-reside on a single TLAN subnet with the Node IP Address.
- Follower cards must reside on the same TLAN subnets.
- All devices must co-reside on the same ELAN subnet as their respective Call Server and node leader.

For dual subnet configuration, make sure the TLAN and ELAN subnets do not overlap.

Example 1 Invalid configuration

The following configuration is not valid, as the TLAN and ELAN subnets overlap.

ELAN network interface:

IP address	10.0.0.136
Subnet mask	255.255.255.128
Default Gateway IP address	10.0.0.129

TLAN network interface:

Node IP address	10.0.0.56
IP address	10.0.0.57
Subnet mask	255.255.255.0
Default Gateway IP address	10.0.0.1

The range of IP addresses in the ELAN subnet – 10.0.0.129 to 10.0.0.255 – overlaps the range of IP addresses in the TLAN subnet – 10.0.0.1 to 10.0.0.255. This contravenes the IP addressing practices, as it is equally valid to route the IP packets over either interface. The resulting behavior from such a setup is undetermined.

The overlapping IP address scheme must be corrected.

Example 2 Valid configuration

The following configuration is valid, as the ELAN and TLAN subnets do not overlap.

The IP addresses can be split as follows.

ELAN network interface:

IP address	10.0.0.136
Subnet mask	255.255.255.128
Default Gateway IP address	10.0.0.129

TLAN network interface:

Node IP address	10.0.0.56
IP address	10.0.0.57
Subnet =mMask	255.255.255.128
Default Gateway IP address	10.0.0.1

The TLAN subnet has a range of addresses from 10.0.0.1 to 10.0.0.127. The ELAN subnet is a separate subnet, with a range of addresses from 10.0.0.129 to 10.0.0.255. This configuration results in a smaller TLAN subnet, but it meets the requirement that subnets do not overlap.

Selecting public or private IP addresses

There are a number of factors to consider when determining if the TLAN and ELAN subnets will use private (internal) IP addresses or public IP addresses.

Private IP addresses

Private, or internal, IP addresses are IP addresses that are not routed over the Internet. They can be routed directly between separate intranets, provided that there are no duplicated subnets in the private IP addresses. Private IP addresses can be used to set up the TLAN and ELAN subnets, so that scarce public IP addresses are used efficiently.

Three blocks of IP addresses have been reserved for private intranets:

- 10.0.0.0 – 10.255.255.255

- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Some routers and firewalls provide a Network Address Translation (NAT) function that allows the customer to map a registered globally-unique public IP address to a private IP address without renumbering an existing private IP address autonomous domain. NAT allows private IP addresses to be accessed selectively over the Internet.

Public IP addresses

Public IP addresses can be used for the TLAN and ELAN subnets, but consume limited resources.

This has the same result as the private IP address solution, but the ELAN subnet is accessible from the IP network without NAT.

ELAN and TLAN network interfaces on a single subnet

IP Trunk 3.0 (or later) supports the use of a single network interface (for example, the ELAN network interface). The CS 1000S system does not have this option.

Single-subnet configuration implies the configuration and use of just one network interface, namely the ELAN network interface, over which all voice and management traffic is routed. Single-subnet configuration can also mean configuring both the TLAN and ELAN network interfaces in the same subnet. Neither configuration is supported. The ELAN and TLAN network interfaces must be assigned IP addresses in different subnets.

Separate or dual subnet configuration implies configuration of both the TLAN and ELAN network interfaces. All management and intra-system signaling traffic is routed out the ELAN network interface, while all telephony traffic is routed out the TLAN network interface.

Note: When using separate subnets as recommended, the Network Activity LEDs provide useful status information regarding the state of the ELAN and TLAN network interfaces. When using an ITG-Pentium 24-port trunk card in a single-subnet configuration, all traffic uses the

ELAN network interface. This eliminates the use of the TLAN network interface.

Although not recommended, the single-subnet configuration of voice and management could be used in the following situations:

- The combined voice and management traffic on the ELAN subnet is so low that there is no impact on packetized voice QoS performance.
- The customer is willing to tolerate occasional voice quality impairments caused by excessive management traffic.

Multiple nodes on the same ELAN and TLAN subnets

There are several configurations where it is acceptable to put multiple nodes on the same dedicated ELAN and TLAN subnets (separate subnets):

- Several nodes belonging to the same customer and related to the same CS 1000 Call Server can be configured to route calls with different CODECs, depending on the digits dialed, or the NCOS of the originating telephone. It can also be configured to limit the maximum number of IP Trunk calls to a particular destination node. The traffic engineering considerations on the TLAN subnet determine how many different nodes can be configured on the same LAN segment.
- Layer 2 (10BaseT or 100Base TX) switching equipment or ATM infrastructure can support a Virtual LAN (VLAN) segment that is distributed across a campus or larger corporate network. In this case, some or all of the ITG destination nodes can be on the same subnet.
- In test labs, training centers, and trade shows, it is common for destination nodes to be located on the same ELAN and TLAN subnets.

Do not place other IP devices, except those designated as acceptable by Nortel, on the ELAN or TLAN subnets.

Guidelines for configuring a routable ELAN subnet

When configuring a routable ELAN subnet on the enterprise IP network, use the following guidelines:

- 1 External multicasts must not be transmitted on the ELAN subnet. Generally, multicast forwarding is disabled by default on a gateway router. Ensure that no multicast routing protocols are enabled on the ELAN subnets gateway router. Do not configure or allow the ELAN or TLAN subnet's gateway router (that is, the Layer 3 switch) to forward multicast traffic to the ELAN subnet.
- 2 External broadcasts must not be forwarded to the ELAN subnet. Ensure that the Layer 3 switch is configured so that it does not forward broadcast traffic from elsewhere on the network to the ELAN subnet. This includes disabling any features on the Layer 3 switch which forward broadcast packets to a subnet when the received packets destination IP address is the subnet's broadcast IP address. This can also include disabling other broadcast-forwarding mechanisms, such as UDP broadcast forwarding, DHCP forwarding, or NetBIOS forwarding.
- 3 An ELAN subnet's gateway router must be capable of Packet Filtering in order to prevent unauthorized traffic from entering the ELAN subnet. Management traffic is sent from management systems to the CS 1000 system. Management traffic includes FTP, Telnet, http, SNMP, DBA, and rlogin servers. Refer to Appendix D for the control and management TCP and UDP port numbers for each component connected to the ELAN subnet. Configure the packet filter to forward any traffic with the source IP address equal to management system's IP address and a management service destination TCP or UDP port. The packet filter should then drop all other traffic.

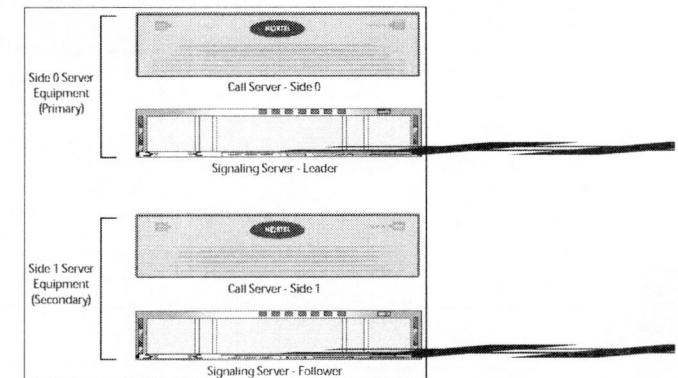
Redundant LAN design

A redundant network has one or more backup systems or elements available for processing or transmission in case of system or element failure.

Single physical location

To begin planning for redundancy, classify equipment into primary and secondary group, as shown in Figure 34 on page 198.

Figure 34
Primary and secondary equipment groups



To implement a redundant core network, follow these recommendations:

- Connect ELAN and TLAN network interfaces for the primary core components (Call Server, leader Signaling Server, and media cards) to the primary Layer 2 switch.
- Connect ELAN and TLAN network interfaces for the secondary core components (Alternate Call Server, Follower Signaling Server, and media cards) to the secondary Layer 2 switch.
- Provide backup power for all essential components and networking devices.
- Use data equipment that supports port-based Virtual LANs (VLANs) and prioritization (IEEE 802.1Q standard).
- Install load-sharing connections or install backup connections, using the or Spanning Tree Protocol (STP), to multiple Layer 3 switches. OSPF is the preferred protocol in this case.

Note: Spanning Tree Protocol convergence can cause Layer 2 switch ports to be disabled for up to 60 seconds. This can affect the entire system.

- If using a highly-available chassis-based system (for example, Passport 8100), designate one card as the primary Layer 2 switch and another card as the secondary Layer 2 switch. Then, group the ELAN and TLAN subnets with port-based VLANs.

Note: Use of a single highly-available Nortel Passport 8600 switch can provide a 'five nines' network.

Figures 35 to through 37 starting on page 200 show a network architecture that divides the core components into primary and secondary devices. Each device is connected to its corresponding Layer 2 switch. Both the ELAN and TLAN network interfaces are connected to the respective Layer 2 switch. VLANs can be used to reduce the number of switches required to obtain a redundant core network.

Figure 35 on page 200 show a redundant core network that does not utilize VLANs on the Layer 2 switch infrastructure.

IMPORTANT!

The primary and secondary TLAN network interfaces must be in the same subnet and broadcast domain.

The primary and secondary ELAN network interfaces must be in the same subnet and broadcast domain

Figure 35
Redundant core network – no VLAN on Layer 2 switch infrastructure

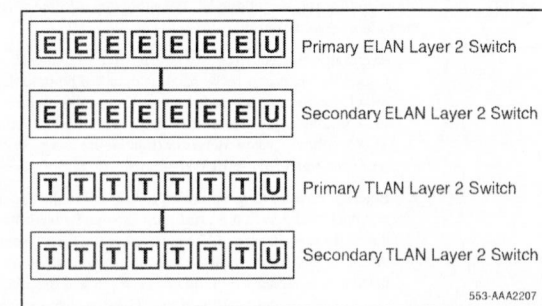
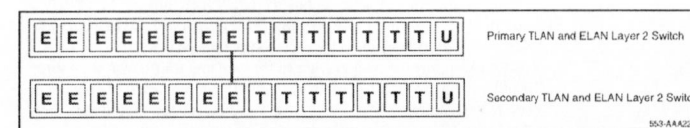


Figure 36 is an example of a redundant core network that does utilize VLANs on the Layer 2 switch infrastructure.

Figure 36
Redundant core network - VLANs on the Layer 2 switch infrastructure



Note: Using VLANs saves using two Layer 2 switches.

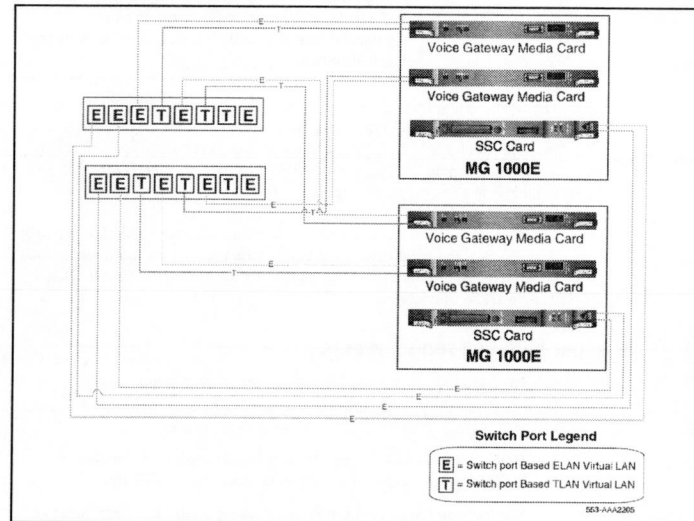
Figure 37 on page 201 shows MG 1000E redundancy details. To obtain maximum redundancy:

- Connect alternate connecting media cards to primary and secondary Layer 2 switches.
- Connect the primary MG 1000E IPDB network interface to the primary Layer 2 switch.

- Connect the secondary IPDB network interface to the secondary Layer 2 switch.

Note: It is possible to locate an MG1000E Elan on a different Layer 3 subnet to that of the Call Server provided that network parameters follow.

Figure 37
MG 1000E redundancy details



CS 1000E Campus redundancy

Figure 38 and Figure 39 on page 203 show campus redundancy for a CS 1000E system. If planning to utilize campus redundancy, follow these recommendations:

- To implement the campus redundant Layer 2 switch configuration, Virtual LANs are required on the Layer 2 switches.
- The Layer 2 switch ports connecting the HSP network interfaces must be in a completely isolated VLAN.
- Group the two gigabit fiber optic links using a multi-link trunk protocol.

Enable Spanning Tree Protocol Fast Port on all switch ports and the multi-link trunk, or disable spanning tree protocol on all switch ports.

Figure 38
Campus redundancy - Layer 2 switch configuration

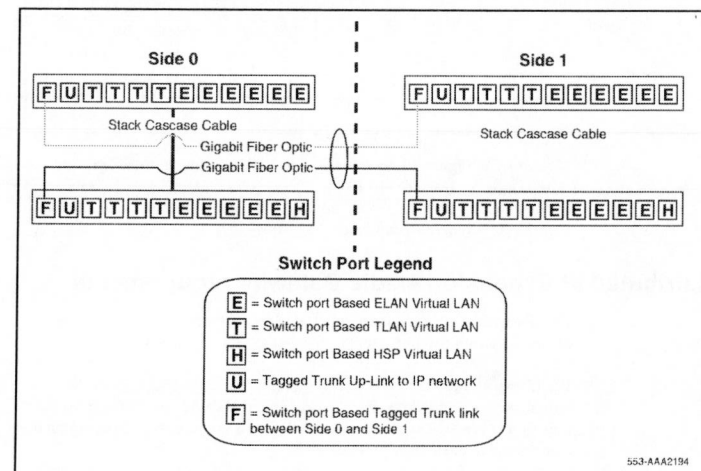
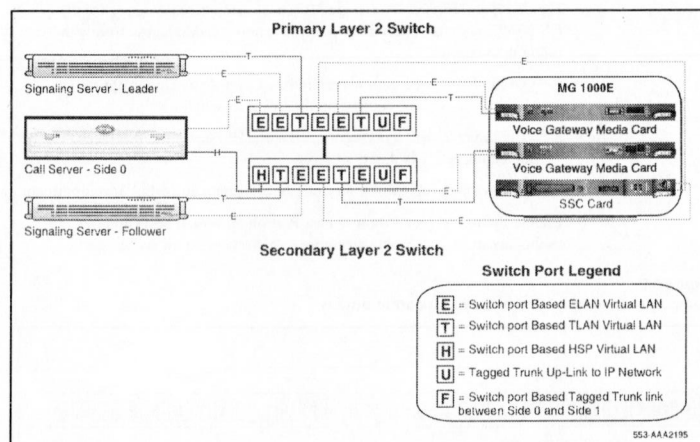


Figure 39
Campus redundancy - Side 0 with VLANs



Note: In Figure 39, Side 0 and Side 1 are considered to be identical.

For detailed information about campus redundancy, refer to *Communication Server 1000: System Redundancy* (553-3001-307).

Distributed IP Expansion Media Gateway requirements

The IP expansion links connect the Call Server IP daughterboards to the Media Gateways Small System Controller (SSC) daughterboards.

The IP expansion links have strict requirements due to the packetization format used over the links. Each packet contains data from multiple users. This format is efficient, but echo cancellation is not possible. To avoid echo, network delay must be very small.



WARNING

Configure the ports on Layer 2 or Layer 3 switching equipment as **Auto-negotiate**.

If one side is manually configured, and the other side is configured as Auto-negotiate, the following situation occurs:

The Auto-negotiate side sets itself to the manually configured side's speed, but always sets itself to half-duplex. If the manually-configured side is full-duplex, then a mismatch occurs, and voice quality is unsatisfactory.

The IP expansion links connect the Call Server to each MG 1000S Small System Controller (SSC) or Media Gateway 1000T (MG 1000T) (see Figure 27 on page 172). In many cases, IP daughter boards are connected using point-to-point cabling (crossover cable) and non-routable IP addresses, but they can also operate through a Layer 2 switch.

The IP expansion links can also be routed across a Layer 3 switched network if the latency and bandwidth requirements are met. Nortel recommends that IPDB network interfaces be connected to a subnet from the ELAN, TLAN, and Nortel Server subnets.

IP expansion link requirements

For the best voice quality, the 100BaseTx IP expansion link from the Call Server's IP daughterboard network interfaces to the IP expansion SSC's IPDB network interface must meet the following requirements:

- 100BaseT Layer 2 (or Layer 3) switch that supports full-duplex connection; software-based routers do not support SIPE links.
- The ports on Layer 2 (or Layer 3) switching equipment must be set to auto-negotiate ENABLED.
- packet loss < 0.5% (0% loss recommended)
- 100 Mbps full-duplex link (minimum)
 - bandwidth usage on an idle system is negligible

- peak bandwidth under high voice traffic conditions (IP Phone to trunk calls) – 21 Mbps
- network delay — Round Trip Delay (RTD) with PDV jitter buffer set to:
 - maximum: < 5 ms
 - minimum: < 12 ms
- support Port Priority Queuing (recommended, but not required)
- support VLAN configuration (recommended, but not required)

Bandwidth planning

CS 1000S and CS 1000M Small Systems are designed for non-blocking transmission between the Call Server and the MG 1000S and CS 1000T systems. The throughput of the network must be guaranteed.

Under high traffic conditions, a peak bandwidth of 21 Mbps is used for voice traffic that requires MG 1000S, such as trunk services. See Table 28.

Note: A minimum 100-Mbps full-duplex link is required.

If there is no traffic flow, bandwidth requirements are negligible. Only active channels use bandwidth.

Table 28
Bandwidth Consumption/100BaseTx (Part 1 of 2)

Number of active conversations	Voice bandwidth (Mbps)	Signaling bandwidth (Mbps)	Total bandwidth (Mbps)
0	0	0.11	0.11
16	5.25	0.5	5.75
32	6.27	0.5	6.77
64	8.32	0.5	8.82

Note: This table applies to voice traffic that requires MG 1000S services.

Table 28
Bandwidth Consumption/100BaseTx (Part 2 of 2)

Number of active conversations	Voice bandwidth (Mbps)	Signaling bandwidth (Mbps)	Total bandwidth (Mbps)
128	12.4	0.5	12.9
256	20.6	0.5	21.1

Note: This table applies to voice traffic that requires MG 1000S services.

Monitoring IP expansion link QoS

Behavior of the network depends on factors like Round Trip Delay (RTD), Packet Delay Variation (PDV) jitter buffers, queuing delay in the intermediate nodes, packet loss, and available bandwidth. The service level of each IP link is measured and maintained on the Call Server.

If using cross-over cables to connect the SIPE daughter boards together, verify the active link.

Information on latency and packet loss is collected from the hardware and processed.

Based on system-configured thresholds, the level of service is compiled and reported by the PRT QOS command in LD 117. See *Software Input/Output: Maintenance* (553-3001-511).

Table 29 provides Data Network Ratings (Excellent, Good, Fair, Poor) and actual parameter values for network delay.

Table 29
SIPE link voice quality measurements (Part 1 of 2)

Voice QoS Rating	Network Round Trip Delay (PDV Max 7.8 ms)	Network Round Trip Delay (PDV Min 0.5 ms)	Network Packet Loss
Excellent	<5 ms	<12 ms	<0.5%
Good	5 – 25 ms	12 – 32 ms	0.5 – 1%

Table 29
SIPE link voice quality measurements (Part 2 of 2)

Voice QoS Rating	Network Round Trip Delay (PDV Max 7.8 ms)	Network Round Trip Delay (PDV Min 0.5 ms)	Network Packet Loss
Fair	25 – 45 ms	32 – 52 ms	1 – 1.5 ms
Poor	>45 ms	>52 ms	>1.5%

The values in Table 29 assume that there is no echo cancellation mechanism and no particular mechanism for recovering lost packets.

IP expansion link Packet Delay Variation jitter buffer

The IP expansion link Packet Delay Variation (PDV) jitter buffer ensures a constant voice playback rate, even when there is variation in the voice packet arrival rate. The PDV jitter buffer is also used to re-sequence out-of-order voice packets, and is integral to the IP-based clock recovery scheme.

The PDV jitter buffer delay is adjustable and should be as short as possible. The minimum and maximum values for excellent voice quality are given in Table 29 on page 206.

Insufficient jitter buffer delay causes a degradation in voice in the form of clicks or pops during a voice call. Insufficient delay is indicated when the QoS monitor reports buffer underflows. If this happens, increase the size of the PDV buffer. Maximize the PDV buffer to minimize round trip delay. The goal is to operate with as smallest possible buffer. Increase the buffer delay in 0.5 ms increments until the QoS monitor no longer reports buffer underflows.



CAUTION

Excessive delay causes a degradation in voice quality in the form of additional echo.

Note: Echo cancellers must be installed wherever the IP network interfaces with a TDM network that uses a 2-wire device, such as an analog loop device.

The command `PRT PDV` in LD 117 displays both the current size of the PDV buffer and the number of PDV underflows.

In addition, a warning message is printed when a parameter threshold (or combination of thresholds) is reached. These thresholds are not user configurable.

The command `CHG PDV` in LD 117 is used to set PDV buffer size on a per-link basis. The command should be run initially using default settings. Then increase its delay parameter in 0.5 ms increments if an unacceptable level of voice quality occurs (pops and clicks). Decrease this value if echo occurs. The goal is to have with the smallest jitter buffer possible.

The PDV jitter buffer size for each IP expansion link is configured at the Call Server and is automatically downloaded to the MG 1000S.

For detailed information on these commands, refer to *Software Input/Output: Maintenance* (553-3001-511).

Distributed Media Gateway 1000E

A Media Gateway 1000E (MG 1000E) can be physically distributed within an enterprise IP network, providing the following criteria are met:

- IPMG's IPDB network interfaces must be connected to the same ELAN subnet as the CS 1000E Call Server.
- Media Cards in the physically-distributed MG 1000E must be connected to the same ELAN subnet as the CS 1000E Call Server. A Layer 2 virtual LAN-enabled campus network architecture can be used to accomplish this.
- Packet loss on the enterprise IP network must be less than 0.5% (0% packet loss is recommended).
- Round-trip delay between Call Server and MG 1000E must be less than 12 ms.

- Use of a QoS mechanism is highly recommended and assists in meeting packet loss and latency requirements.

Campus-distributed Media Gateway enhancements

The Media Gateway enhancement allows the Campus Media Gateway 1000E to be on a separate subnet from the Call Server and traverse a Layer 3 routing protocol, and enables the Campus Media Gateway 1000E to use any Layer 2 switch. The Campus Redundancy enhancement enables the ELAN network interface connections of the various nodes to reside on different subnets. Therefore, the following is no longer necessary:

- Signaling Server ELAN network interface IP address to reside on the same subnet as the IP address of the Voice Gateway Media Card's ELAN network interface
- Call Server IP address (ELAN network interface) to reside on the same subnet as the IP address of the Voice Gateway Media Card's ELAN network interface

This enhancement also changes the operation of the ELAN subnet between the Call Server and the Media Gateway 1000Es. It allows the Media Gateway 1000Es to be on a different subnet than the Call Server.

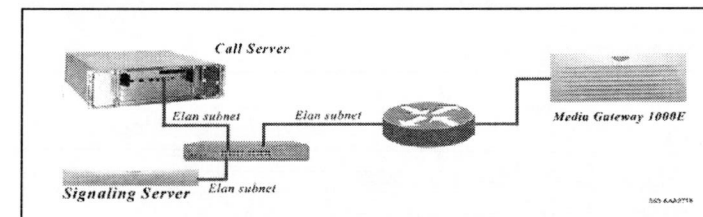
Previously, the installation of Media Gateway 1000Es required that the ELAN subnet and broadcast domain be extended to any Media Gateway 1000E installed in the campus, exposing the Call Server subnet to Layer 2 traffic, including broadcasts, from the customer network. Signaling to the Voice Gateway Media Card ELAN network interfaces requires this VLAN, due to messages that are broadcast to all devices on the ELAN subnet; specifically, the messages sent after a warm start or cold start are broadcast over the ELAN subnet to inform all devices how to handle their existing media paths and connections. Signaling to the Small System Controller (SSC) of the Media Gateway 1000E does not require such a VLAN connection, since these messages are provided using Layer 3 IP routing.

This enhancement propagates the SSC messages for warm start and cold start to all devices within the SSC's broadcast domain, if the subnet of the SSC is different than that of the Call Server. This allows the Voice Gateway Media

Card ELAN network interfaces to receive this information without having a VLAN connection back to the Call Server.

The Media Gateway enhancement provides the additional functionality to separate the Call Server/Signaling Server ELAN subnet from the Media Gateway 1000E through a Layer 3 routing protocol. See Figure 40.

Figure 40
Media Gateway separation from the Call Server by Layer 3 router



Operating parameters

IP Phones are not supported on remote Media Gateway1000Es (Media Gateway1000Es that are separated from the Call Server by Layer 3 routing).

Campus-distributed Media Gateway 1000E IP address configuration

If the Voice Gateway Media Card ELAN network interface and its associated Call Server are not on the same subnet and VLAN/broadcast domain, then for signaling to reach the Call Server, ensure the following:

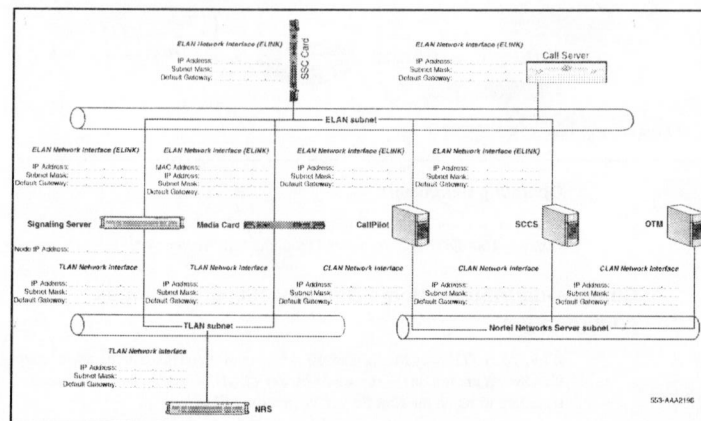
- The Management LAN (ELAN) Gateway IP address configured in CS 1000 Element Manager is propagated to all Voice Gateway Media Cards in the node.
- The routing is properly configured to allow routing through a Layer 3 IP network between the Voice Gateway Media Card ELAN network interface and the Call Server.

When Media Gateway 1000Es are distributed through an IP network without a VLAN connection to the Call Server, configure the Voice Gateway Media Card ELAN network interfaces on the same subnet as the MG1000E Small System Controller (SSC) 100BaseT network interface. This allows broadcasts from the SSC to reach the Voice Gateway Media Cards.

Sample system layout

Figure 41 shows a sample system layout for the CS 1000S.

Figure 41
CS 1000S sample system layout



Address and connection tables

The following tables can be used to record address and connection records for:

- system servers — use Table 30 on page 212

- Media Gateway 1000T (MG 1000T) — Table 31 on page 214
- applications — Table 32 on page 218

System server addresses and connections

Use Table 30 to record system server addresses and connections.

Table 30
System servers addresses and connections (Part 1 of 2)

System IP addresses	
Node IP address:	
Primary NRS IP address:	
Alternate NRS IP address:	
SNMP NRS IP address:	
Call Server 0 (ELNK)	
ELAN network interface	
IP address:	
Subnet Mask:	
Default Gateway:	
Call Server 1 (ELNK)	
ELAN network interface	
IP address:	
Subnet Mask:	
Default Gateway:	
Signaling Server	
ELAN network interface	
IP address:	
Subnet Mask:	

Table 30
System servers addresses and connections (Part 2 of 2)

Default Gateway:	
<i>TLAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
IPMG SSC	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
Voice Gateway Media Card	
<i>ELAN network interface</i>	
MAC address:	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>TLAN network interface</i>	
Node IP address:	
IP address:	
Subnet Mask:	
Default Gateway:	

Media Gateway 1000T addresses and connections

Use Table 31 to record MG 1000T addresses and connections.

Table 31
MG 1000T addresses and connections (Part 1 of 4)

System IP addresses	
Node IP address:	
Primary NRS IP address:	
Alternate NRS IP address:	
SNMP NMS IP address:	
SSC 0	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>IPM 1 network interface</i>	
IP address:	
Subnet Mask:	
<i>IPM 2 network interface</i>	
IP address:	
Subnet Mask:	
<i>IPM 3 network interface</i>	
IP address:	
Subnet Mask:	

Table 31
MG 1000T addresses and connections (Part 2 of 4)

<i>IPM 4 network interface</i>	
IP address:	
Subnet Mask:	
SSC 1	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>IPR 1 network interface</i>	
MAC address:	
IP address:	
Subnet Mask:	
SSC 3	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>IPR 3 network interface</i>	
MAC address:	
IP address:	
Subnet Mask:	

Table 31
MG 1000T addresses and connections (Part 3 of 4)

SSC 2	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>IPR 2 network interface</i>	
MAC address:	
IP address:	
Subnet Mask:	
SSC 4	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>IPR 4 network interface</i>	
MAC address:	
IP address:	
Subnet Mask:	
Signaling Server	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	

Table 31
MG 1000T addresses and connections (Part 4 of 4)

<i>TLAN network interface</i>	
Node IP address:	
IP address:	
Subnet Mask:	
Default Gateway:	
Voice Gateway Media Card	
<i>ELAN network interface</i>	
MAC address:	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>TLAN network interface</i>	
Node address:	
IP address:	
Subnet Mask:	
Default Gateway:	

Application addresses and connections

Use Table 32 to record application addresses and connections.

Table 32
Application addresses and connections (Part 1 of 2)

CallPilot Server	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>CLAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
SSCS	
<i>ELAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	
<i>CLAN network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	

Table 32
Application addresses and connections (Part 2 of 2)

OTM Server	
<i>network interface</i>	
IP address:	
Subnet Mask:	
Default Gateway:	

Operating the VoIP network

Contents

This section contains information on the following topics:

System management	221
OTM	222
Element Manager	222
Network monitoring	223
Set VoIP QoS objectives	224
Intranet QoS monitoring	225
ITG Operational Measurements	226
OM report description	227
User feedback	227
QoS monitoring and reporting tools	228
Network Diagnostic Utilities	229
Proactive Voice Quality Management	241
Network Management	251
SNMP Network Management Systems	251
OTM and Network Management System	251
Policy Management	252
CS 1000 network inventory and configuration	252

System management

The system can be managed using Optivity Telephony Manager (OTM) or CS 1000 Element Manager.

OTM

Optivity Telephony Manager (OTM) is an integrated suite of system management tools. Compatible with a standard PC, it provides a single point of access and control to manage the systems.

OTM uses IP technology to target the following:

- single point of connectivity to the system and related devices
- data collection for traffic and billing records
- collection, processing, distribution, and notification of alarms and events
- data propagation
- performance measurement tools (Traffic Analysis package, and Real-time Conferencing Protocol (RTCP) statistics from the Terminal Proxy Server (TPS) and Voice Gateway Media Cards)
- web-based management applications, including security

OTM can be integrated with the suite of Optivity management tools to provide comprehensive management of the voice and data network.

For more information about OTM, refer to *Optivity Telephony Manager: Installation and Configuration* (553-3001-230) or *Optivity Telephony Manager: System Administration* (553-3001-330)

Element Manager

Element Manager is a simple and user-friendly web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, D-channels)

- maintenance commands, system status inquiries, backup and restore functions
- software download, patch download, patch activation

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single point-of-access to parameters that were traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.
- The hide or show information option enables administrators to see information that relates directly to the task at hand.
- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.
- Configuration screens offer pre-selected defaults, drop-down lists, checkboxes, and range values to simplify response selection.

The Element Manager web server resides on the Signaling Server and can be accessed directly through a web browser or Optivity Telephony Manager (OTM). The OTM navigator includes integrated links to each network system and their respective instances of Element Manager.

For more information on using Element Manager, refer to *Element Manager: System Administration* (553-3001-332).

Network monitoring

The network design process is ongoing, continuing after implementation of the VoIP network and commissioning of voice services over the network. Network changes VoIP traffic, general intranet traffic patterns, network policies, network topology, user expectations, and networking technology can render a design obsolete or non-compliant with QoS objectives. Review the design periodically against prevailing and trended network conditions and traffic patterns, at least once every two to three weeks initially, then on a quarterly basis.

It is assumed that the customer's organization already has processes in place to monitor, analyze, and re-design both the Meridian Customer Defined Network (MCDN) and the corporate intranet, so that both networks continue to conform to internal QoS standards. When operating VoIP services, the customer's organization must incorporate additional monitoring and planning processes, such as:

- Collect, analyze, and trend VoIP traffic patterns.
- Monitor and trend one-way delay and packet loss.
- Monitor Operational Measurements (see page 226).
- Perform changes in VoIP network and intranet when planning thresholds are reached.

By implementing these new processes, the VoIP network can be managed to meet desired QoS objectives.

Set VoIP QoS objectives

State the design objective of the VoIP network. This sets the standard for evaluating compliance to meeting users' needs. When the VoIP network is first installed, the design objective expectations have been set based on the work done in "Network performance evaluation overview" on page 102.

Initially, set the QoS objective so that for each destination pair, the mean+ σ of one-way delay and packet loss is below some threshold value to maintain calls between those two sites at a required QoS level. The graphs in Figure 20 on page 106 and Figure 21 on page 107 help determine what threshold levels are appropriate.

Table 33 on page 225 describes examples of VoIP QoS objectives.

Table 33
VoIP QoS objectives

Site Pair	IP Trunk 3.0 (or later) QoS objective	Fallback threshold setting
Santa Clara/ Richardson	Mean (one-way delay) + s (one-way delay) < 120 ms Mean (packet loss) + s (packet loss) < 0.3%	Excellent
Santa Clara/ Ottawa	Mean (one-way delay) + s (one-way delay) < 120 ms Mean (packet loss) + s (packet loss) < 1.1%	Excellent

In subsequent design cycles, review and refine the QoS objective based on data collected from intranet QoS monitoring.

After deciding on a set of QoS objectives, determine the planning threshold based on the QoS objectives. These thresholds are used to trigger network implementation decisions when the prevailing QoS is within range of the targeted values. This gives time for implementation processes to follow through. Set the planning thresholds 5% to 15% below the QoS objectives, depending on the implementation lag time.

Intranet QoS monitoring

To monitor one-way delay and packet loss statistics, install a delay and route monitoring tool, such as PING and Traceroute on the TLAN of each IP Trunk 3.0 (or later) site. Each delay monitoring tool runs continuously, injecting probe packets to each ITG site about every minute. The amount of load generated by this is not considered significant. At the end of the month, the hours with the highest one-way delay are noted; for those hours, the packet loss and standard deviation statistics can be computed.

At the end of the month, analyze each site's QoS information. Table 34 on page 226 provides a sample.

Table 34
QoS monitoring

Site pair	One-way delay Mean+s (ms)		Packet loss Mean+s (%)		QoS		
	Last period	Current period	Last period	Current period	Last period	Current period	Objective
Santa Clara/ Richardson	135	166	1	2	Excellent	Good	Excellent
Santa Clara/ Ottawa	210	155	3	1	Good	Excellent	Excellent

Declines in QoS can be observed through the comparison of QoS between the last period and current period. If a route does not meet the QoS objective, take immediate action to improve the route's performance.

See "Network performance measurement tools" on page 108 for information about how to obtain other more specialized delay and route monitoring tools.

ITG Operational Measurements

The Voice Gateway Media Card collects Operational Measurements (OM) from the IP Phones and DSP channels and saves the information to a log file every 60 minutes. The Operational Measurements include:

- IP Phone Registration Attempted Count
- IP Phone Registration Confirmed Count
- IP Phone Unregistration Count
- IP Phone Audio Stream Set Up Count
- IP Phone Average Jitter (ms)
- IP Phone Maximum Jitter (ms)
- IP Phone Packets Lost/Late (%)
- IP Phone Total Voice Time (minutes and seconds)
- Gateway Channel Audio Stream Set Up Count

- Gateway Channel Average Jitter (ms)
- Gateway Channel Maximum Jitter (ms)
- Gateway Channel Packets Lost/Late (%)
- Gateway Channel Total Voice Time (minutes and seconds)

OM report description

The OM log file is a comma-separated (.csv) file stored on the OTM server. Use OTM to run an ad hoc report, or schedule a regular report. A new file is created for each month of the year in which OM data is collected. It can be read directly, or imported to a spreadsheet application for post-processing and report generation. Collect these OM reports and store them for analysis. At the end of each month, identify the hours with the highest packet lost/late statistics and generate standard deviation statistics. Compare the data to target network QoS objectives.

Declining QoS can be observed by comparing QoS between periods. A consistently inferior measurement of QoS compared to the objective triggers an alarm. The customer must take steps to strengthen the performance of the route. The card creates a new log file each day. Files are automatically deleted after seven days.

User feedback

Qualitative feedback from users helps to confirm if the theoretical QoS settings match what end users perceive. The feedback can come from a Help Desk facility and must include information such as time of day, origination and destination points, and a description of service degradation.

The fallback threshold algorithm requires a fixed IP Trunk 3.0 (or later) system delay of 93 ms, which is based on default IP Trunk 3.0 (or later) settings and its delay monitoring probe packets. The fallback mechanism does not adjust when IP Trunk 3.0 (or later) parameters are modified from their default values. Users can perceive a lower quality of service than the QoS levels at the fallback thresholds in the following situations:

- Delay variation in the intranet is significant. If the standard deviation of one-way delay is comparable with the voice playout maximum delay, it

means that there is a population of packets that arrive too late to be used by the IP Trunk 3.0 (or later) node in the playout process.

- The jitter buffer is increased. In this case, the actual one-way delay is greater than that estimated by the delay probe.
- The CODEC is G.711A or G.711U. The voice packets formed by these CODECs are larger (120 to 280 bytes) than the delay probe packets (60 bytes). This means there is greater delay experienced per hop. If there are low-bandwidth links in the path, the one-way delay is noticeably higher in average and variation.

QoS monitoring and reporting tools

These tools are used in the post-installation, day-to-day activities of maintaining an acceptable QoS level for the VoIP network. Passive tools are used to monitor and report on real-time VoIP traffic metrics gathered from network devices that already collect and gather RMON information.

To adequately assess the data network on an on-going basis, other more intrusive tools are used to generate synthetic VoIP traffic. The more intrusive tools are similar to those used to perform pre-sales network assessments.

Nortel recommends customers use a mechanism that provides notification of QoS policy breaches through e-mail, alarm, or page. The ability of these tools to generate timely reports on QoS is also important. The QoS data is copied from holding registers into a Management Information Base (MIB) at each recording interval; therefore, the customer must periodically secure the data before it is refreshed at the next interval.

Available tools

Some examples of QoS monitoring and reporting tools include:

- NetIQ Chariot™
- RMON
- MultiRouter Traffic graphing tool
- SNMP NMS traffic reports

For more detailed information regarding specific QoS assessment, monitoring and reporting tools available, contact your Nortel sales representative.

Network Diagnostic Utilities

Network diagnostic utilities are accessible on Phase II IP Phones to isolate voice quality problems. The diagnostic utilities can be run from the menu-driven interface of the IP Phone itself. Refer to *IP Phones: Description, Installation, and Operation* (553-3001-368) for details on running the diagnostic utilities on the IP Phone.

The diagnostic utilities are also available at the OAM prompt of the Signaling Server Command Line Interface (CLI). Table 35 on page 231 describes the network diagnostic CLI commands, and indicates if they are available in Element Manager.

Ping and Traceroute

The system administrator can execute a Ping or Traceroute command from a specific endpoint with any arbitrary destination, typically another endpoint or Signaling Server. The CLI commands are:

- **rPing** — Requests IP Phone to ping a specified IP address.
- **rPingStop** — Requests IP Phone to stop pinging a specified IP address.
- **rTraceRoute** — Requests IP Phone to trace route a specified IP address.
- **rTraceRouteStop** — Requests IP Phone to stop tracing the route a specified IP address.

IP Networking statistics

The system administrator can view information on the packets sent, packets received, broadcast packets received, multicast packets received, incoming packets discarded, and outgoing packets discarded. Use the CLI command **eStatShow** to display Ethernet statistics for a specified IP Phone.

Ethernet statistics

The system administrator can view ethernet statistics (for example, number of collisions, VLAN ID, speed and duplex) for the IP Phone on a particular

endpoint. The exact statistics will depend on what is available from the IP Phone for the specific endpoint.

UNISTIM/RUDP statistics

The system administrator can view RUDP statistics (for example, number of messages sent, received, retries, resets, and uptime) for the IP Phones. Use the CLI command **RUDPStatShow** to display RUDP statistics:

Real-time Transport Protocol statistics

The system administrator can view RTP/RTCP QoS metrics (for example, packet loss, jitter, and R-value) while a call is in progress. The CLI commands are:

- **RTPTraceShow** — Displays RTP/RTCP statistics for an IP endpoint (icid if the endpoint is a Voice Gateway Media Card). This command can be active across all calls, and can show statistics for multiple intervals.
- **RTPTraceStop** — Requests issuing IP endpoint to stop RTPTraceShow.
- **RTPStatShow** — Displays RTP/RTCP statistics.

DHCP

The system administrator can view DHCP settings (for example, IP address, S1, S2, and S4 addresses) for each IP Phone. Use the CLI command **isetInfoShow** to display standard DHCP configuration information, set firmware version, hardware identification and server information of an IP Phone.

Table 35
Network diagnostic CLI commands (Part 1 of 10)

Command	Available in Element Manager
Description rPing <TN IP>, <dest>[, <count>] Request IP Phone to ping an IP address, where: <TN IP> = TN or IP address of set issuing Ping <dest> = destination IP address <count> = number of successful ping responses the pinging set should receive. If this count is not specified, it is fixed to 4. Example: <pre>oam> rping 47.11.215.153, 47.11.216.218, 5</pre> 56 bytes packets received from IP 47.11.216.218. 5 packets transmitted, 5 packets received, 0 packets lost minim round trip time in ms: 0.1ms average round trip time in ms: 0.2 ms maximum round trip time in ms: 0.4ms rPingStop <TN IP> Request issuing IP Phone to stop ping.	Yes No

Table 35
Network diagnostic CLI commands (Part 2 of 10)

Command	Available in Element Manager
Description rTraceRoute <TN IP>, <dest>, <count> Request specified IP Phone to trace the route of a destination IP address. Where: <TN IP> = TN or IP address of set issuing rTraceRoute <dest> = the destination IP address <count> = maximum number of hops Example: <pre>oam> rTraceRoute 47.11.215.153, 47.11.174.10, 6</pre> <pre>1 -- 47.11.181.3 1.079ms 0.768ms 0.744ms</pre> <pre>2 -- 47.11.174.10 2.681ms 2.654ms 2.690ms</pre> <pre>3 -- * * *</pre> <pre>4 -- * * *</pre> <pre>5 -- * * *</pre> <pre>6 -- last packet</pre> rTraceRouteStop <TN IP> Request issuing IP Phone to stop route trace.	Yes No

Table 35
Network diagnostic CLI commands (Part 3 of 10)

Command	Available in Element Manager
Description RUDPStatShow <TN IP> [, <clear>] Display information received from an IP endpoint. Displayed information includes number of messages sent, number of messages received, and number of retries. If specified, the statistics are cleared before display. Where: <TN IP> = TN or IP address of an IP Phone <clear> = Clear counts of messages sent, messages received, and number of retries, where: 0 = Does not clear the statistics (default) 1 = Clears the statistics and displays zero counts. Example – do not clear statistics: <pre>oam> RUDPStatShow 47.11.215.153</pre> Messages sent: 309 Messages received: 321 Number of retries: 10 Uptime of current TPS registration: 2 hour 24 minutes 35 seconds Example – clear statistics: <pre>oam> RUDPStatShow 47.11.215.153, 1</pre> Messages sent: 0 Messages received: 0 Number of retries: 0 Uptime of current TPS registration: 2 hour 24 minutes 35 seconds	No

Table 35
Network diagnostic CLI commands (Part 4 of 10)

Command	Available in Element Manager
Description eStatShow <TN IP> [, <clear>] Display Ethernet information received from an IP endpoint. If specified, the statistics are cleared before they are displayed. Displayed information includes: • interface speed and duplex mode • Auto negotiate protocol received/not received • VLAN ID and priority • packet collisions (peg count) • CRC errors (peg count) • framing errors (peg count) Where: <TN IP> = TN or IP address of an IP endpoint. <clear> = Clears counts of packet collisions, CRC errors, and framing errors, where: 0 = Does not clear the statistics (default) 1 = Clears the statistics and displays zero counts. Example – do not clear statistics: <pre>oam> eStatShow 47.11.215.153</pre> 100 base T full duplex Auto negotiate protocol received VLAN ID: 88 Priority: 1 Packet collisions: 100 CRC errors: 30 Framing Errors:1	No

Table 35
Network diagnostic CLI commands (Part 5 of 10)

Command	Available in Element Manager
Example – clear statistics: <pre>oam> eStatShow 47.11.215.153, 1 100 base T full duplex Auto negotiate protocol received VLAN ID: 88 Priority: 1 Packet collisions: 0 CRC errors: 0 Framing Errors:0</pre>	

Table 35
Network diagnostic CLI commands (Part 6 of 10)

Command	Available in Element Manager
isetInfoShow <TN IP> Display standard DHCP configuration information, set firmware version, hardware identification and server information of an IP Phone. Where: <TN IP> = TN or IP address of the IP Phone. Example: <pre>oam> isetInfoShow 47.11.215.153 FW Version: 0602B50 HWID: 18006038DD1ADB6600 MAC: 006038DD1ADB VLAN ID: 124 Priority: 6 Set IP: 47.103.225.125 Subnet Mask: 255.255.255.0 Set Gateway: 47.103.225.1 LTPS IP: 47.103.247.224 Node IP: 47.103.247.224 Node ID: 4420 S1 Node IP: 47.103.247.229 Port: 4100 Action: 1 S2 Node IP: 47.103.247.229 Port: 4100 Action: 1 S5 Node IP: 47.103.247.229 Port: 4100 XAS: Net6</pre>	Yes

Table 35
Network diagnostic CLI commands (Part 7 of 10)

Command	Available in Element Manager
RTPStatShow <TN IP> Display QoS polling information. Where: <TN IP> = TN or IP address of the IP Phone. Example: Note: The output lines in this example are truncated to fit in the available space; each line of output is actually prefixed by the following: RTPStatShow Report (RTCP-XR) from Set (164.164.8.20) <pre>oam> RTPStatShow 164.164.8.20 Far End IP address: 164.164.8.21 Far End Port: 5200 Local Packet Sent: 2978 Local Packet Received: 2535 Local Packet Received out of order: 0 Local Pkt Loss: 14% Local Average Jitter: 0ms Local Latency: 9ms Local Listening R: 63 Vocoder Type: 0 Local Avg Net Loss Rate: 14.79% Local Avg Discard Rate: 0.00% Local Avg Burst Density: 17.11% Local Avg Burst Length: 2070ms Local Gap Density: 10.34% Local Gap Length: 1080ms Local Avg End System Delay: 15ms Local Avg Noise Level: 0dBm Local Avg Signal Power: 0dBm Local Round Trip Time Avg: 19ms Local Round Trip Time Avg High: 19ms</pre>	Yes

Table 35
Network diagnostic CLI commands (Part 8 of 10)

Command	Available in Element Manager
<pre>Remote Listening R: 0 Remote Avg Net Loss Rate: 0% Remote Avg Discard Rate: 0% Remote Avg Burst Density: 0% Remote Avg Burst Length: 0ms Remote Gap Density: 0% Remote Gap Length: 0ms Remote Avg End System Delay: 0ms Remote Avg Noise Level: 0dBm Remote Avg Signal Power: 0dBm Remote Round Trip Time Avg: 0ms Remote Round Trip Time Avg High: 0ms Remote Packet Loss: 0% Remote Average Jitter: 0ms Remote Latency: 0ms</pre>	

Table 35
Network diagnostic CLI commands (Part 9 of 10)

Command	Available in Element Manager
Description RTPTraceShow <TN IP> [, <polling period>] Display RTP/RTCP statistics for an IP endpoint. This command can be active across all calls. Where: <TN IP> = TN or IP address of the endpoint (tcid if the endpoint is a Voice Gateway Media Card) <polling period> = Number of polling periods to be displayed. If not specified, default is 10 polling periods. Example: Note: The output lines in this example are truncated to fit in the available space; each line of output is actually prefixed by the following: RTPTraceShow Report from Set (164.164.8.20) <pre>oam> RTPTraceShow 164.164.8.20 Far End IP address: 164.164.8.21 Far End Port: 5200 Far End IP address: 164.164.8.21 Far End Port: 5200 Local Packet Sent: 2978 Local Packet Received: 2535 Local Packet Received out of order: 0 Local Pkt Loss: 14% Local Average Jitter: 0ms Local Latency: 9ms Local Listening R: 63 Vocoder Type: 0</pre>	No

Table 35
Network diagnostic CLI commands (Part 10 of 10)

Command	Available in Element Manager
Description Local Avg Net Loss Rate: 14.79% Local Avg Discard Rate: 0.00% Local Avg Burst Density: 17.11% Local Avg Burst Length: 2070ms Local Gap Density: 10.34% Local Gap Length: 1080ms Local Avg End System Delay: 15ms Local Avg Noise Level: 0dBm Local Avg Signal Power: 0dBm Local Round Trip Time Avg: 19ms Local Round Trip Time Avg High: 19ms Remote Listening R: 0 Remote Avg Net Loss Rate: 0% Remote Avg Discard Rate: 0% Remote Avg Burst Density: 0% Remote Avg Burst Length: 0ms Remote Gap Density: 0% Remote Gap Length: 0ms Remote Avg End System Delay: 0ms Remote Avg Noise Level: 0dBm Remote Avg Signal Power: 0dBm Remote Round Trip Time Avg: 0ms Remote Round Trip Time Avg High: 0ms Remote Packet Loss: 0% Remote Average Jitter: 0ms Remote Latency: 0ms RTPTraceStop Request issuing IP endpoint to stop RTPTraceShow.	No

For information on network diagnostic utilities, refer to *IP Phones: Description, Installation, and Operation* (553-3001-368) and *Signaling Server: Installation and Configuration* (553-3001-212).

Proactive Voice Quality Management

For Communication Server 1000 Release 4.5 (and later), Proactive Voice Quality Management (PVQM) assists system administrators to:

- make informed decisions for capacity planning, and QoS network engineering
- monitor the performance of their system
- diagnose, isolate, and correct networking problems that cause deterioration in voice quality

PVQM is supported by CS 1000 and Meridian 1 systems equipped with Voice Gateway Media Cards running IP Line 4.0 (or later). PVQM includes the following:

- monitoring of voice quality metrics (for example, latency, jitter, packet loss, and R-Value) for IP Phones and gateway endpoints

Note: Monitoring of R-Value available on Phase II IP Phones only. To enable monitoring of the R-Value audio quality metric, the Proactive Voice Quality Management (PVQM) package 401 is required.

- two levels of voice quality alarms (for example, Warning and Unacceptable). Alarm thresholds, configured in LD 117, are used to classify system performance as good, poor, and unacceptable.

Note: Available on Phase II IP Phones only.

- SNMP alarm generation when voice quality metric thresholds are violated on a per-call or bandwidth-zone basis
- controlling the number of voice quality-related SNMP alarms (on a zone-by-zone basis) by configuring zone alarm notification in LD 117. Alarm control assists in isolating voice quality problems and reducing network traffic.
- recording of voice quality metric threshold violations, accessible in IP Phone Zone Traffic Report 16 (LD 2) and SNMP MIB

Note: IP Phone Zone Traffic Report 16 (TFS016) includes peg counts for both alarm levels (that is, Warning and Unacceptable) when recording voice quality metric threshold violations for latency, jitter, and packet loss. R-Value is limited to one peg count (that is, Unacceptable).

- R-Value information is available in Operational Measurement (OM) reports. OM reports contain hourly summations of voice quality metrics and endpoint registration activity.
- network diagnostic utilities to identify, isolate, and report network problems affecting voice quality. The diagnostic utilities are available by using the Command Line Interface (CLI) or IP Phones with Phase II software. The utilities include Traceroute, Ping, Ethernet statistics, IP Network statistics, UNISim/RUDP statistics, RTCP statistics, and DHCP data. See "Network Diagnostic Utilities" on page 229.

How voice quality monitoring works

The PVQM feature monitors voice quality by measuring the following:

- **Latency** - length of time for information to travel through the network, in seconds
- **Jitter** - variability in latency, in seconds
- **Packet Loss** - number of packets lost during transmission, in percentage
- **R-Value** - measurement of listening R-Value using ITU E-Model. R-Value maps to Mean Opinion Score (MOS).

The sampled metrics are compared to user-configured thresholds in order to determine system performance. When sampled metrics exceed configured thresholds, statistics are generated on the system.

Note: For details on configuring metric thresholds, refer to "Configure voice quality metric thresholds" on page 247.

Statistics for each metric are collected on the Signaling Server or Voice Gateway Media Card to create a traffic report. The traffic report classifies metric threshold violation peg counts as Warning or Unacceptable.

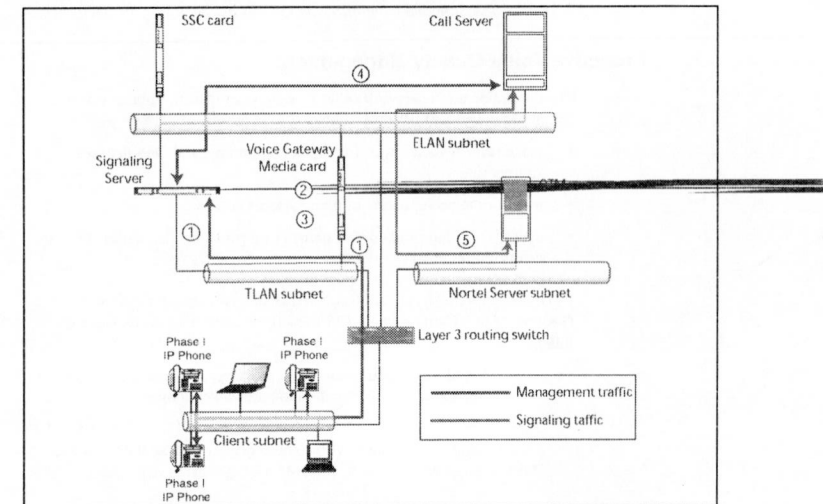
Each summarized traffic report is added to the IP Phone Zone Traffic Report 16 (TFS016), which in turn summarizes voice quality over the reporting period on a zone-by-zone basis. IP Phone Zone Traffic Report 16 (TFS016) provides the system administrator with an overall view of voice quality on the system. For information on IP Phone Zone Traffic Report 16 (TFS016), refer to *Traffic Measurement: Formats and Output* (553-3001-450).

An SNMP alarm is generated when a voice quality metric threshold exceeds Warning or Unacceptable status. For details on controlling the number of SNMP alarms generated, refer to "Configure and print zone alarm notification levels" on page 248.

Phase I IP Phones voice quality monitoring

Figure 42 on page 244 shows voice quality monitoring for Phase I IP Phones within the VoIP system.

Figure 42
Phase I IP Phones voice quality monitoring flow diagram



Referring to Figure 42, the following occurs with Phase I IP Phones:

- 1 Phase I IP Phones and endpoints are polled during. And at the end of, a call to extract voice quality statistics.
- 2 Statistics are collected on the Signaling Server or Voice Gateway Media Card.
- 3 Voice quality statistics are compared to threshold settings. If a threshold is exceeded, the Signaling Server or Voice Gateway Media Card generates an initial SNMP alarm.

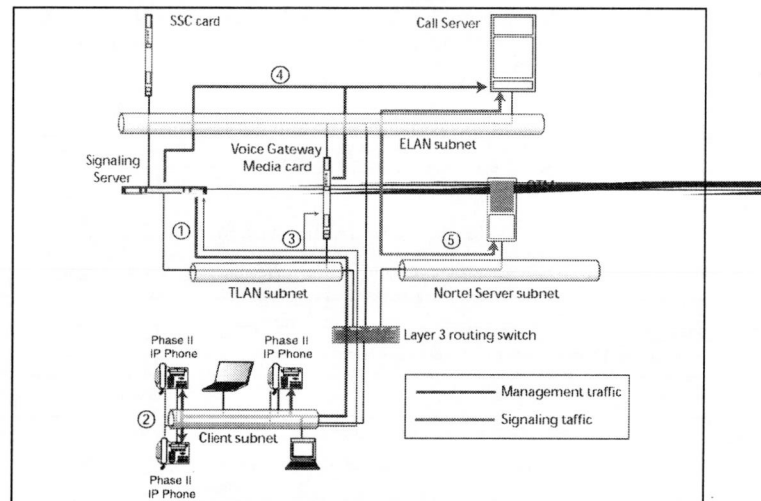
For voice quality metric alarms that reach the Unacceptable level, the path (tracert) of the voice media is written to the log file on the Signaling Server or Voice Gateway Media Card for diagnostic purposes.

- 4 Call quality information and alarm alert is forwarded to the Call Server.
- 5 The Call Server generates a second SNMP alarm.

Phase II IP Phones voice quality monitoring

Figure 43 shows voice quality monitoring for Phase II IP Phones within the VoIP system.

Figure 43
Phase II IP Phones voice quality monitoring flow diagram



Referring to Figure 43, the following occurs with Phase II IP Phones:

- 1 The Signaling Server sends pre-set threshold values to the Phase II IP Phone.
- 2 Statistics are collected and compared on the Phase II IP Phone.

- 3 When a threshold is exceeded, the Phase II IP Phone sends an alert to the Signaling Server or Voice Gateway Media Card, which generates an initial SNMP alarm.

For voice quality metric alarms that reach the Unacceptable level, the path (tracert) of the voice media is written to the log file on the Signaling Server or Voice Gateway Media Card for diagnostic purposes.

- 4 Call quality information and alarm alert is forwarded to the Call Server.
- 5 The Call Server generates a second SNMP alarm.

Voice quality alarms

Table 36 identifies metrics, threshold levels, alarming severity, and QoS alarms for the following categories:

- Call Server alarms on a call-by-call basis
- Call Server alarms aggregated by zone
- Signaling Server (LTPS) alarms

Table 36
Call Server alarms - Call-by-call (Part 1 of 2)

Metric	Threshold level	Severity	Alarms
Call Server alarms - Call-by-call			
Latency, Jitter, Packet Loss, R-Value	Warning	Info	QOS0001 - QOS0005 (excluding QOS0004)
Latency, Jitter, Packet Loss, R-Value	Unacceptable	Minor	QOS0007 - QOS0010
Call Server alarms - Aggregated by zone			
Latency, Jitter, Packet Loss, R-Value	Warning	Minor	QOS0012 - QOS0015
Latency, Jitter, Packet Loss, R-Value	Unacceptable	Critical	QOS0017 - QOS0020
Signaling Server (LTPS) alarms			
Latency, Jitter, Packet Loss, R-Value	Warning	Warning	QOS0022, QOS0024, QOS0026, QOS0028

Table 36
Call Server alarms - Call-by-call (Part 2 of 2)

Metric	Threshold level	Severity	Alarms
Latency, Jitter, Packet Loss, R-Value	Unacceptable	Minor	QOS0030, QOS0032, QOS0034, QOS0036
Latency, Jitter, Packet Loss, R-Value	Clear	Clear	QOS0023, QOS0027, QOS0029, QOS0031, QOS0033, QOS0035, QOS0037

For information on QoS alarms, refer to *Software Input/Output: System Messages* (553-3001-411).

Configure voice quality metric thresholds

The system administrator can configure and print voice quality metric thresholds on a per-call or zone basis. Use the following commands in LD 117:

- **CHG CQWTH** — Change voice quality Warning thresholds on a per call basis.
- **CHG CQUTH** — Change voice quality Unacceptable thresholds on a per call basis.
- **CHG ZQWTH** — Change voice quality Warning thresholds on a zone basis.
- **CHG ZQUTH** — Change voice quality Unacceptable thresholds on a zone basis.
- **PRT QSTHS** — Display all voice quality thresholds.

For detailed information on these commands, refer to *Software Input/Output: Maintenance* (553-3001-511).

Configure voice quality sampling (polling)

Use the **CHG SQOS** command in LD 117 to configure the sampling (polling) period, zone-alarm-rate collection window, and the minimum number of samples to collect during the window.

For detailed information on these commands, refer to *Software Input/Output: Maintenance* (553-3001-511).

Configure and print zone alarm notification levels

Systems that process a large number of calls potentially generate a significant number of SNMP alarms. Controlling the number of alarms by configuring zone alarm notification levels helps isolate voice quality problems and reduce network traffic.

Voice quality threshold alarms are examined for their severity relative to the alarm notification level settings. If the voice quality threshold alarm severity exceeds the configured notification level, it generates an SNMP alarm; otherwise, the alarm is suppressed.

Voice quality threshold alarm notification levels can be set on a zone-by-zone basis so that some bandwidth zones can be monitored for all alarms and other zones will report only serious voice quality problems. Alarm notification levels are defined in Table 37 on page 248.

Table 37
Voice quality threshold alarm notification levels (Part 1 of 2)

Level	Description	Alarms
0	All voice quality alarms are suppressed	None
1	Allow zone-based Unacceptable alarms	QOS0017, QOS0018, QOS0019, QOS0020
2	Allow all of the above PLUS zone-based Warning alarms	All of the above PLUS, QOS0012, QOS0013, QOS0014, QOS0015

Table 37
Voice quality threshold alarm notification levels (Part 2 of 2)

Level	Description	Alarms
3	Allow all of the above PLUS per-call Unacceptable alarms	All of the above PLUS, QOS0007, QOS0008, QOS0009, QOS0010, QOS0032, QOS0033, QOS0036, QOS0037
4	Allow all of the above PLUS per-call Warning alarms	All of the above PLUS, QOS0001, QOS0002, QOS0003, QOS0005, QOS0018, QOS0019, QOS0022, QOS0023, QOS0024, QOS0025, QOS0026, QOS0027

The system administrator controls the number of alarms generated by the system using the **CHG ZQNL** alarm notification level configuration commands. The system administrator can print alarm notification levels using the **PRT ZQNL** command. Both commands are in LD 117.

For detailed information on these commands, refer to *Software Input/Output: Maintenance* (553-3001-511).

Heterogeneous environments

In an environment with a mixture of Nortel equipment and third-party equipment, voice-quality monitoring, detection, and alarming is performed only on IP endpoints that have voice quality monitoring capabilities.

For information on IP endpoints and their voice quality capabilities in the system, refer to Table 38 on page 250.

Table 38
IP Endpoint and voice quality capabilities

Endpoint type	Voice quality monitoring operation
Phase 0/I IP Phones	Detects jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Threshold violations are detected by polling.
Phase II IP Phones without PVQM package 401	Detects jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Threshold violations are detected asynchronously by the IP Phone.
Phase II IP Phones with PVQM package 401	Detects jitter, packet loss, and latency (when the far end is RTCP-compliant) and R-Value threshold violations. Threshold violations are detected asynchronously by the IP Phone.
IP Softphone 2050	Detects jitter, packet loss, and latency (when the far end is RTCP-compliant) threshold violations. Threshold violations are detected by polling.
CS 1000 and Meridian 1 systems with Voice Gateway Media Cards running IP Line 4.0 (and later)	Detects jitter and packet loss threshold violations. Threshold violations are detected by polling.
Third-party Gateway	Not supported

Network Management

SNMP Network Management Systems

Simple Network Management Protocol (SNMP)-based Network Management Systems (NMS) monitors a real-time network from end-to-end. This is important for VoIP networks. NMS ensures that problems on a network running real-time traffic are solved quickly to maintain high-quality service.

SNMP NMS software can be configured to perform the following actions:

- map the network
- monitor network operation through polling of network devices
- centralize alarm management through SNMP traps
- notify network administrators of problems

The CS 1000 system can be integrated into an NMS to provide a complete view of the converged voice and data network. Problems can be isolated much more quickly when looking at the entire network.

SNMP Agent support is provided in OTM 1.1 and later. This allows alarms sent from devices to be forwarded to the NMS.

Nortel also provides a complete line of Enterprise Network management software with the Optivity Enterprise Network Management Solutions product line. An SNMP interface is available in the traffic reporting system so that OTM, or any third-party system, can have a standards-based interface into the system traffic reports. Refer to *Simple Network Management Protocol: Description and Maintenance* (553-3001-519).

OTM and Network Management System

OTM can be combined with Optivity Network Management System (Optivity NMS) Release 9.01, and later. This provides an integrated data, voice, and video network, as part of Unified Networking system. The result is integrated LAN, WAN, and voice network management.

Optivity NMS is an enterprise-level network management solution, providing fault, performance, configuration, and security management for Nortel internetworking devices. Optivity NMS enables network administrators to monitor and manage the network through a single view, and access any Optivity NMS server in the network from one client installation. It provides system-level management instead of managing one device at a time. Optivity NMS provides graphical views from physical connections between the LANs and WANs to the logical connections of a VLAN.

OTM server activity can be monitored through Optivity NMS.

OTM Alarm Manager receives Simple Network Management Protocol (SNMP) traps from managed elements. Through Alarm Notification, OTM sends filtered traps to Optivity NMS.

Policy Management

Policy Management simplifies network QoS configuration by managing network QoS policies from a central location.

Details such as Layer 2, Layer 3, Layer 4, and trust configurations can be implemented for the entire network from a central location. A variety of policy managers are usually available from the network equipment vendor.

The Common Open Policy Services (COPS) protocol is used to transmit standard policies to the network devices.

For more details on Nortel Optivity Policy Services, contact your Nortel representative.

CS 1000 network inventory and configuration

Record the current CS 1000 design and log all additions, moves, and changes that occur in the CS 1000 network. The following information must be recorded:

- CS 1000 site information
 - location
 - dialing plan

- IP addressing
- Provisioning of CS 1000 nodes
 - number of cards and ports
- CS 1000 node and card parameters
 - fallback threshold level
 - CODEC image
 - voice and fax payload
 - voice and fax playout delay
 - audio gain, echo canceller tail delay size, Silence Suppression threshold
 - software version

Appendix A: Subnet mask conversion from CIDR to dotted decimal format

Subnet masks are expressed in Classless InterDomain Routing (CIDR) format, appended to the IP address, such as 10.1.1.1/20. The subnet mask must be converted from CIDR format to dotted decimal format in order to configure IP addresses.

The CIDR format expresses the subnet mask as the number of bits counting from the most significant bit of the first IP address field. A complete IP address consists of 32 bits. Therefore, a typical CIDR format subnet mask is in the range from /9 to /30. Each decimal number field in the dotted decimal format has a value from 0 to 255, where decimal 255 represents binary 1111 1111.

Follow the steps in Procedure 9 to convert a subnet mask from CIDR format to dotted decimal format.

Procedure 9 Converting a subnet mask from CIDR format to dotted decimal format

- 1 Divide the CIDR format value by 8.

The result is a quotient (a zero or a positive number) and a remainder between 0 and 7.

- 2 The quotient designates the number of dotted decimal fields containing 255.

In the example above, the subnet mask in CIDR format is "/20". Twenty divided by eight equals a quotient of two, with a remainder of four. Therefore, the first two fields of the subnet mask in dotted decimal format are 255.255.

- 3 Use Table 39 to obtain the dotted decimal value for the field following the last field containing 255.

In the example of /20 above, the remainder is four. In Table 39, a remainder of four equals a binary value of 1111 0000 and the dotted decimal value of the next field is 240. Therefore the first three fields of the subnet mask are 255.255.240.

- 4 The last field in the dotted decimal format has a value of 0. Therefore, the complete subnet mask in dotted decimal format is 255.255.240.0.

End of Procedure

Table 39
CIDR format remainders

Remainder of CIDR format value divided by eight	Binary value	Dotted decimal value
0	0000 0000	0
1	1000 0000	128
2	1100 0000	192
3	1110 0000	224
4	1111 0000	240
5	1111 1000	248
6	1111 1100	252
7	1111 1110	254

Appendix B: Port number tables

Contents

This section contains information on the following topics:

Introduction	257
Call Server port numbers	258
Signaling Server port numbers	261
IP Line port numbers	264
IP Trunk port numbers	266
Internet Telephony Gateway (ITG) port numbers	267
OTM port numbers	268
IP Phone 200x port numbers	269
Remote Office port numbers	269
CallPilot port numbers	270
Symposium port numbers	274
TLAN subnet stateless packet filtering	275
TLAN subnet stateful packet filtering	276
ELAN subnet packet filtering	278

Introduction

This appendix contains port number tables for all Meridian 1, CS 1000S, and CS 1000M VoIP products.

All ports specified in the following tables are "Listen" ports. That is, these tables specify the destination IP address and destination port number. The tables do not specify the source IP address or port.

The Task column specifies the software task listening on the specified port.

Call Server port numbers

Where:

MGMT = Management

SC = System Control

Table 40
Call Server port numbers (Part 1 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
MGMT	TCP	21	any	FTP	
SC	TCP	111	any	sunrpc - portmapper for RPC	
MGMT	TCP	513	any	rlogin	used by OTM
SC	TCP	1013	any	proprietary	
SC	TCP	1017	any	proprietary	
SC	TCP	1019	any	proprietary	
SC	TCP	1022	any	proprietary	
SC	TCP	2010	qu0	CEMUX related	
SC	TCP	3312	ipDB-	proprietary	
SC	TCP	3313	ipDB-	proprietary	
SC	TCP	7734	any	DTP	
SC	TCP	8888	any	elan / aml	
SC	TCP	15000	any	cs link	
SC	TCP	15080	any	Xmsg Server	for CS 1000 Element Manager

Table 40
Call Server port numbers (Part 2 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SC	TCP	32780	ipDB-	IPDB CLAN	
SC	TCP	32781	ipDB-	SSD	
SC	TCP	32782	ipDB-	Rx IPDB CEMUX	
SC	TCP	32783	ipDB-	proprietary	
SC	TCP	32784	any	IPDB TTY	
SC	TCP	32784	ipDB-	IPDB TTY	
SC	UDP	67	any	bootp	for IP daughterboards
SC	UDP	69	any	tftp	
SC	UDP	111	any	sunrpc - portmapper	
MGMT	UDP	161	any	SNMP	
MGMT	UDP	1929	any	DBA	
SC	UDP	5020	HSP	HSP stop and copy	
SC	UDP	15000	qu0	rudp?	
SC	UDP	32779	any	IPDB HB	
SC	UDP	1003	any		CP-P11; CP PIV
SC	UDP	1004	any	proprietary	CP-P11; CP PIV
SC	UDP	1005	any		CP-P11; CP PIV
SC	UDP	1006	any		CP-P11; CP PIV
SC	UDP	1007	any		CP-P11; CP PIV
SC	UDP	1025	any		CP-P11; CP PIV
SC	UDP	1026	any		CP-P11; CP PIV

Table 40
Call Server port numbers (Part 3 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SC	UDP	2049	any		CP-P11; CP PIV
SC	UDP	5010	any		CP-P11; CP PIV
SC	UDP	5018	any		CP-P11; CP PIV
SC	UDP	17185	any		CP-P11; CP PIV
SC	TCP	993	any		CP-P11; CP PIV
SC	TCP	996	any		CP-P11; CP PIV
SC	TCP	5007	any		CP-P11; CP PIV
SC	TCP	998	any		CP-P11; CP PIV
SC	TCP	1000	any		CP-P11; CP PIV

Signaling Server port numbers

Where:

MGMT = Management

SC = System Control

Table 41
Signaling Server port numbers (Part 1 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
MGMT	TCP	21	any	FTP	
MGMT	TCP	23	any	Telnet	
MGMT	TCP	80	any	http	
SC	TCP	111	any	sunrpc - portmapper	
MGMT	TCP	443	any	https	
MGMT	TCP	513	any	rlogin	
VoIP Signaling	TCP	1720	TLAN	H.323	listens on TLAN IP address
VoIP Signaling	TCP	1720	TLAN	H.323	listens on node IP address
SC	TCP	1024	ELAN	CS link	initiated connection on random port
SC	TCP	1009	any	proprietary	
SC	UDP	16080	any	xmsg server	for element management
SC	UDP	67	any	bootp	

Table 41
Signaling Server port numbers (Part 2 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
Firmware Download	UDP	69	any	tftp	for firmware
SC	UDP	111	any	sunrpc - portmapper	
MGMT	UDP	161	ELAN	SNMP query	
MGMT	UDP	162	any	SNMP trap	
VoIP Signaling	UDP	1718	TLAN	H.323	
VoIP Signaling	UDP	1719	TLAN	H.323	
VoIP Signaling	UDP	1719	TLAN	H.323	
VoIP Signaling	UDP	4100	TLAN	UNISlim	IP Phone 2004
VoIP Signaling	UDP	5100	TLAN	UNISlim	IP Phone 2004
VoIP Signaling	UDP	7300	TLAN	UNISlim	IP Phone 2004
VoIP Signaling	UDP	10000	TLAN	Echo Server	NAT
SC	TCP	1313	any	database synchronization	
SC	TCP	4789	any		
SC	UDP	15000	ELAN	rdp to CS	
SC	UDP	15001	any	rdp to CS?	

Table 41
Signaling Server port numbers (Part 3 of 3)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
VoIP Signaling	UDP	16500	any	Network Connect Server	
SC	UDP	16540	any		proprietary
VoIP Signaling	UDP	16502	any	Network Connect Server	
VoIP Signaling	UDP	16501	any	Network Connect Server	main office listen for branch office
SC	UDP	16550	any	election	
SC	UDP	20001	any	sntp	
VoIP Signaling	TCP	5060	any	SIP	SIP signaling ports
VoIP Signaling	UDP	5060	any	SIP	SIP signaling ports
Firmware Download	UDP	5105	TLAN	UFTP	UNISim File Transfer Protocol

IP Line port numbers

Where:

MGMT = Management

SC = System Control

Table 42
IP Line port numbers (Part 1 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
MGMT	TCP	21	any	FTP	
MGMT	TCP	23	any	Telnet	
SC	TCP	111	any	sunrpc - portmapper	
SC	TCP	1006	any		proprietary
SC	TCP	1009	any		proprietary
SC	TCP	1041	ELAN	cs link	initiated connection on random port
SC	UDP	67	any	bootp	
Firmware Download	UDP	69	any	tftp	
SC	UDP	111	any	sunrpc - portmapper	
MGMT	UDP	161	ELAN	SNMP	
SC	UDP	514	any		proprietary
SC	UDP	15000	ELAN	rdp to CS	
SC	UDP	15001	any		proprietary
SC	UDP	16543	any	intercard sig	
SC	UDP	16550	any	election?	

Table 42
IP Line port numbers (Part 2 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
SC	UDP	20001	any	sntp	
SC	UDP	20777	any		
VoIP Media	UDP	5201 -5263	TLAN	RTCP	odd numbers - Media Card
VoIP Media	UDP	5200 - 5262	TLAN	RTP	even numbers - Media Card
VoIP Media	UDP	5201 - 5247	TLAN	RTCP	odd numbers - ITGP
VoIP Media	UDP	5200 - 5246	TLAN	RTP	even numbers - ITGP

IP Trunk port numbers

Where:

MGMT = Management
SC = System Control

Table 43
IP Trunk port numbers (Part 1 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
VoIP Signaling	TCP	1720	TLAN	H.225	
SC	TCP	6001	ELAN	DCHIP inter-card messaging	
SC	UDP	67	ELAN	BOOTP Server (on Leader Card)	
MGMT	UDP	161	ELAN	SNMP	
VoIP Media	UDP	5000	TLAN	Network QoS monitor port	
VoIP Signaling	UDP	15000	TLAN	MCDN Call Independent Messaging	
VoIP Media	UDP	17300 - 17362	TLAN	RTP	(17300+TCID*2)
VoIP Media	UDP	17301 - 17363	TLAN	RTCP	(17300+TCID*2)
SC	UDP	2001 - 2002	TLAN	Inter-card communication	

Table 43
IP Trunk port numbers (Part 2 of 2)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
VoIP Media	UDP	2300 - 2362	TLAN	RTP	(2300+TCID*2)
VoIP Media	UDP	2301 - 2363	TLAN	RTCP	(2300+TCID*2+1)

Internet Telephony Gateway (ITG) port numbers

Table 44
ITGW port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
ITGW	TCP	1720, 1723	TLAN	(H.225/H.245)	signaling
ITGW	TCP	variable	TLAN	H.225	random port range by RADvision stack H.225 control channel
ITGW	UDP	161	TLAN	SNMP	
ITGW	UDP	1718, 1719	TLAN	H.323 RAS	signaling
ITGW	UDP	2000, 2001	TLAN	inter-card messaging	
ITGW	UDP	2300 - 2346	TLAN	RTP	(2300+TCID*2)
ITGW	UDP	2301 - 2347	TLAN	RTCP	(2300+TCID*2+1)

OTM port numbers

Where MGMT = Management

Table 45
OTM port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
MGMT	TCP	80	any	http	WebCS, DesktopServices, WebTBS
MGMT	TCP/UDP	135	any	Login	RPC SCM used by DCOM
MGMT	TCP	139	any	NetBEUI	Windows client file sharing
MGMT	UDP	162	any	SNMP	Alarm traps (LD117), MaintWindows
MGMT	TCP	1583	any	Btrieve	Station Admin
MGMT	UDP	1929	any	DBA	Call Server
MGMT	TCP	3351	any	Btrieve	Station Admin
MGMT	TCP	5099	any	RMI	OTM DECT
MGMT	TCP	4789 - 5045	any	Virtual System Terminal	

IP Phone 200x port numbers

Table 46
IP Phone 200x port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	UDP	4100	Ethernet	UNISTim	is the TPS
	UDP	variable	Ethernet	RTP	specified by the TPS
	UDP	5000	Ethernet	Net 6	
	UDP	5200	Ethernet	RTP	src from phone
	UDP	5201	Ethernet	RTCP	src from phone

Remote Office port numbers

Table 47
Remote Office port numbers

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
Remote Office	TCP	12800	TLAN	signaling	
Remote Office	UDP/RTP	20480, 20482	TLAN	RTP	voice

CallPilot port numbers

Table 48
CallPilot port numbers (Part 1 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	21	CLAN/ ELAN	FTP	
	TCP	25	CLAN/ ELAN	SMTP	
	TCP	80	CLAN/ ELAN	WWW	
	TCP	135	CLAN/ ELAN	Location Service	
	UDP	135	CLAN/ ELAN	Location Service	
	TCP	137	CLAN/ ELAN	NETBIOS Name Service	
	UDP	137	CLAN/ ELAN	NETBIOS Name Service	
	TCP	138	CLAN/ ELAN	NETBIOS Datagram Service	
	TCP	139	CLAN/ ELAN	NETBIOS Session Service	
	TCP	143	CLAN/ ELAN	IMAP2	
	UDP	161	CLAN/ ELAN	SNMP (if enabled)	
	UDP	162	CLAN/ ELAN	SNMP-trap (if enabled)	

Table 48
CallPilot port numbers (Part 2 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	389	CLAN/ ELAN	LDAP	
	TCP	443	CLAN/ ELAN	http over SSL	
	TCP	465	CLAN/ ELAN	SSMTP (Secure SMTP)	
	TCP	636	CLAN/ ELAN	LDAP over SSL	
	TCP	1025	CLAN/ ELAN	msdtc	
	TCP	1026	CLAN/ ELAN	msdtc	
	TCP	1027	CLAN/ ELAN	Microsoft Distribute COM Services	
	TCP	1028	CLAN/ ELAN	Microsoft Distribute COM Services	
	TCP	1029	CLAN/ ELAN	Dialogic CTMS	
	TCP	1030	CLAN/ ELAN	Dialogic CTMS	
	TCP	1031	CLAN/ ELAN	Dialogic CTMS	
	TCP	1032	CLAN/ ELAN	Dialogic CTMS	

Table 48
CallPilot port numbers (Part 3 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	1036	CLAN/ ELAN	CallPilot Middleware Maintenance Service Provider	
	TCP	1037	CLAN/ ELAN	CallPilot Call Channel Resource	
	TCP	1038	CLAN/ ELAN	CallPilot Multimedia Resource	
	TCP	1039	CLAN/ ELAN	CallPilot MCE Notification Service	
	TCP	1040	CLAN/ ELAN	CallPilot MCE Notification Service	
	TCP	1041	CLAN/ ELAN	CallPilot MCE Notification Service	established connection to local ports 2019
	TCP	1042	CLAN/ ELAN	CallPilot MTA	established connection to local ports 2019
	TCP	1045	CLAN/ ELAN	CallPilot Access Protocol	established connection to local ports 2019
	TCP	1046	CLAN/ ELAN	CallPilot SLEE	established connection to local ports 2019
	TCP	1047	CLAN/ ELAN	IIS	

Table 48
CallPilot port numbers (Part 4 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	1048	CLAN/ ELAN	IIS	
	TCP	1095	CLAN/ ELAN	CallPilot Blue Call Router	
	TCP	1096	CLAN/ ELAN	CallPilot Blue Call Router	established connection to local ports 2019
	TCP	1148	CLAN/ ELAN	TAPI	established connection to port 8888 on the switch
	TCP	2019	CLAN/ ELAN	Dialogic CTMS	established connection to local ports 1041, 1042, 1045, 1046, 1096
	TCP	2020	CLAN/ ELAN	Dialogic CTMS	
	TCP	5631	CLAN/ ELAN	pcAnywhere data	
	UDP	5632	CLAN/ ELAN	pcAnywhere stat	
	TCP	7934	CLAN/ ELAN	IIS	
	TCP	8000	CLAN/ ELAN	Dialogic CTMS	
	TCP	10008	CLAN/ ELAN	CallPilot Access Protocol	

Table 48
CallPilot port numbers (Part 5 of 5)

Task	L4 protocol (TCP/UDP)	Port number or range	Interface	Description	Comments
	TCP	38037	CLAN/ ELAN	msgsys Intel CBA-Message System	
	TCP	56325	CLAN/ ELAN	CallPilot SLEE	

Symposium port numbers

For Symposium port numbers, refer to Symposium documentation.

TLAN subnet stateless packet filtering

Table 49 describes a stateless packet filtering configuration. The primary intent of this configuration is to secure management access the CS 1000 system using the TLAN subnet.

These rules are for the TLAN subnet only. IP Phones are assumed to be deployed on client subnets throughout the IP network. All other TCP and UDP ports running on the TLAN network interfaces are for system control traffic which should not be sent through the packet filter. Optionally, drop all management traffic into the TLAN subnet.

Table 49
TLAN subnet - Stateless packet filtering configuration

Rule #	Task (App/Interface)	Source IP add.	Source TCP/UDP port	Dest. IP add.	Protocol type	Dest. TCP/UDP port	Action	Description
System Management								
1	System MGMT	MGMT	ignore	TLAN subnet	any	any	Forward	Allow MGMT System
2	System MGMT	any	ignore	TLAN subnet	TCP	21	Drop	FTP
3	System MGMT	any	ignore	TLAN subnet	TCP	23	Drop	Telnet
4	System MGMT	any	ignore	TLAN subnet	TCP	80	Drop	http Element Management
5	System MGMT	any	ignore	TLAN subnet	TCP	111	Drop	RPC
6	System MGMT	any	ignore	TLAN subnet	UDP	162	Drop	SNMP
7	System MGMT	any	ignore	TLAN subnet	TCP	513	Drop	rlogin
Firewall								
8	Default Rule	any	ignore	TLAN subnet	UDP	any	Forward	Default Action

TLAN subnet stateful packet filtering

Table 50 describes rules for a stateful firewall only; they do not apply to a non-stateful firewall. IP Phones are assumed to be deployed on client subnets throughout the IP network. All other TCP and UDP ports running on the TLAN network interfaces are for system control traffic, which should not be sent through the packet filter. Optionally, drop all management traffic into the TLAN subnet.

Table 50
TLAN subnet - stateful packet filtering (Part 1 of 2)

Rule #	Task (App/Interface)	Source IP add.	Source TCP/UDP port	Dest. IP add.	Protocol type	Dest. TCP/UDP port	Action	Description
System Management								
1	System MGMT	MGMT	ignore	TLAN subnet	TCP	21	Forward	FTP
2	System MGMT	MGMT	ignore	TLAN subnet	TCP	23	Forward	Telnet
3	System MGMT	MGMT	ignore	TLAN subnet	TCP	80	Forward	Element Manager
4	System MGMT	MGMT	ignore	TLAN subnet	TCP	513	Forward	rlogin
VoIP Signaling								
5	SigSvr / Gatekpr	any	ignore	TLAN subnet	TCP	1720	Forward	H.323 Signaling
6	SIP	any	ignore	TLAN subnet	TCP	5060	Forward	SIP Signaling (configurable)
7	Firmware Download	any	ignore	TLAN subnet	UDP	69	Forward	TFTP
8	H.323	any	ignore	TLAN subnet	UDP	1718	Forward	H.323 Signaling
9	H.323	any	ignore	TLAN subnet	UDP	1719	Forward	H.323 Signaling
10	TPS	any	ignore	TLAN subnet	UDP	4100	Forward	IP Phone 200x signaling

Table 50
TLAN subnet - stateful packet filtering (Part 2 of 2)

Rule #	Task (App/Interface)	Source IP add.	Source TCP/UDP port	Dest. IP add.	Protocol type	Dest. TCP/UDP port	Action	Description
11	SIP	any	ignore	TLAN subnet	UDP	5060	Forward	SIP Signaling (configurable)
12	TPS	any	ignore	TLAN subnet	UDP	5100	Forward	IP Phone 200x signaling (configurable)
13	Firmware Download	any	ignore	TLAN subnet	UDP	5105	Forward	UNISim FTP
14	TPS	any	ignore	TLAN subnet	UDP	7300	Forward	IP Phone 200x signaling
15	Virtual Office	any	ignore	TLAN subnet	UDP	16500	Forward	Virtual Office signaling (Network connect server configurable)
16	Virtual Office	any	ignore	TLAN subnet	UDP	16501	Forward	Virtual Office Signaling
VoIP Media								
17	SMC	any	ignore	TLAN subnet	UDP	5200-5263	Forward	RTP/RTCP voice media
18	System MGMT	MGMT	ignore	TLAN subnet	UDP	162	Forward	SNMP
Firewall								
19	Firewall	any	ignore	TLAN subnet	ignore	any	Drop	Default Action

ELAN subnet packet filtering

Table 51 describes a packet filtering configuration suitable for a routable ELAN subnet. These filters are effective for stateless and stateful packet filters.

Table 51
ELAN subnet - packet filtering

Rule #	Task (App/Interface)	Source IP add.	Source TCP/UDP port	Dest. IP add.	Protocol type	Dest. TCP/UDP port	Action	Description
System Management								
1	System MGMT	MGMT	Ignore	ELAN subnet	TCP	21	Forward	FTP
2	System Magma	MGMT	Ignore	ELAN subnet	TCP	23	Forward	Telnet
3	System Magma	MGMT	Ignore	ELAN subnet	TCP	80	Forward	http Element Management
4	System Magma	MGMT	Ignore	ELAN subnet	TCP	513	Forward	rlogin
7	System Magma	MGMT	Ignore	ELAN subnet	UDP	162	Forward	SNMP query
8	System Magma	MGMT	Ignore	ELAN subnet	UDP	1929-2185	Forward	DBA for OTM
System Signaling								
9	System Signaling	CC6	ignore	Call Server	TCP	8888	Forward	CC6 AML Link
Note: Rule 9 applies only to a system with a Contact Center 6 system using a single network interface to the Nortel server subnet.								
Firewall								
9	Firewall	any	Ignore	ELAN subnet	ignore	any	Drop	Default action

Appendix C: DHCP supplemental information

Contents

This section contains information on the following topics:

Introduction to DHCP	279
DHCP messages	280
DHCP message format	281
DHCP message exchange	282
DHCP options	282
Vendor Specific/Encapsulated option	283
Site Specific option	283
IP acquisition sequence	284
Case 1	284
Case 2	286
Case 3	287
Multiple DHCPOFFERS	287
IP Phone support for DHCP	288
Full DCHP	288
Partial DCHP	293
DHCP Auto Discovery	294s

Introduction to DHCP

To understand how the IP Phones 200x and the IP Softphone 2050 acquire the needed network configuration parameters automatically, the following section briefly describes the Dynamic Host Configuration Protocol (DHCP).

Read this section unfamiliar with DHCP. Topics discussed are helpful for the configuration and future maintenance of the DHCP server and ensure correct implementation with IP Phones.

DHCP is an extension of BootP. Like BootP, it operates on the client-server model. However, DHCP has more message types than BootP. DHCP enables the dynamic allocation of IP addresses to different clients. It can be used to configure clients by supplying the network configuration parameters such as gateway or router IP addresses.

In addition, DHCP has a lease system that controls the duration an IP address is leased to a client. The client can request a specific lease length, or the administrator can determine the maximum lease length. A lease can range from one minute to 99 years. When the lease is up or released by the client, the DHCP server automatically retrieves it and reassigns it to other clients, if necessary. This is an efficient and accurate way to configure clients quickly. This saves the administrator from an otherwise repetitive task. IP addresses can be shared among clients that do not require permanent IP addresses.

DHCP messages

There are seven different DHCP messages. Each message relays certain information between the client and server. See Table 52.

Table 52
DHCP message types (Part 1 of 2)

DHCP Message Types	Description
DHCPDISCOVER	Initiates a client request to all servers.
DHCPOFFER	Offer from server following client request.
DHCPREQUEST	Requests a particular server for services.
DHCPACK	Notifies client that requested parameters can be met.
DHCPNAK	Notifies client that requested parameters cannot be met.

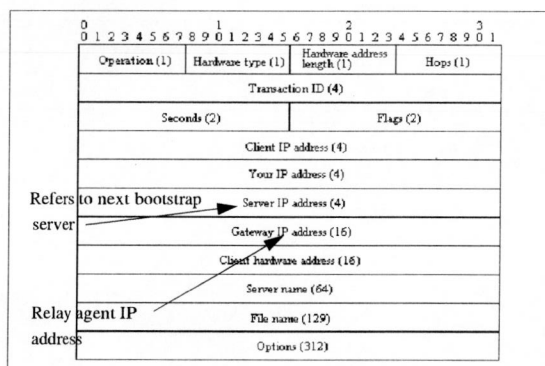
Table 52
DHCP message types (Part 2 of 2)

DHCP Message Types	Description
DHCPDECLINE	Notifies server that offer is unsatisfactory and will not be accepted.
DHCPRELEASE	Notifies server that IP address is no longer needed.

DHCP message format

The DHCP message format shown in Figure 44 is common to all DHCP messages. Each message consists of 15 fields: 14 fixed-length fields and one variable length field. The fixed-length fields must be the specified number of bytes, as indicated in the brackets. If there is not enough data, or there is no data at all, zeros are used to fill in the extra spaces.

Figure 44
DHCP message format



The Options field is the only field with a variable length. It is optional, but very important, as it transports additional network configuration parameters. The DHCP options are the actual subfields that are used in this project.

DHCP message exchange

For a client to receive services from a DHCP server, an exchange of DHCP messages between the client and server must take place. The sequence and types of DHCP message exchanged can differ, but the mechanism of acquiring and supplying information remains the same.

Usually the client initiates the exchange with a DHCP message broadcast. Using a broadcast enables the client to send messages to all servers on the network without having an associated IP address. The broadcast is local to the LAN, unless a DHCP relay agent is present to forward the packet.

At this point, the client has no information about the server or the IP address it is going to receive (unless it is requesting a renewal), so the fields in the DHCP message are empty. However, the client knows its own MAC address and includes it in the Client hardware address field. The client can also have a list of parameters it would like to acquire and can request them from the DHCP server by including the Parameter Request List option (Option Code 55) in the DHCPDISCOVER message.

When the DHCP server sees the broadcast, it responds by broadcasting its own DHCP message. The server, since it knows more about the network, is able to fill in most of the information in the message. For example, information such as the server IP address and gateway IP address are included in their respective fields. Since the client does not have an IP address yet, the server uses the client's MAC address to uniquely identify it. When the client sees the broadcast, it matches its MAC address against the one in the message.

DHCP options

DHCP options are the sub-fields of the Options field. They carry additional network configuration information requested by the client such as the IP address lease length and the subnet mask.

Each DHCP option has an associated option code and a format for carrying data. Usually the format is as follows:

Option code Length Data

There are two categories of DHCP options: standard and non-standard. The standard options are predefined by the industry. The non-standard options are user-defined to fit the needs of a particular vendor or site.

There are a total of 255 DHCP option codes where option codes 0 and 255 are reserved, 1 – 77 are predefined, 1 – 254 can be used for Vendor Specific Options, and 128 – 254 are designated for Site Specific Options. This arrangement enables future expansion and is used as a guideline for choosing option codes.

Vendor Specific/Encapsulated option

The Vendor Specific DHCP options are vendor-defined options for carrying vendor-related information. It is possible to override predefined standard options; however, doing so can cause conflict when used with components that follow the industry standard.

A useful option is the standard Vendor Encapsulated option – code 43. It is used to encapsulate other DHCP options as sub-options. For example, the IP Phone 2004 requires vendor specific Voice Gateway Media Card information. The vendor, Nortel, decided to carry this information in one of several Site Specific options and then encapsulate it into option 43. Since the information is specific to a Nortel product, it is vendor-specific. Once encapsulated, the information appears as one or more sub-options inside option 43, which the IP Phone decodes.

Site Specific option

Another way to transport the Voice Gateway Media Card information is through Site Specific options. These are unused DHCP options that have not been predefined to carry standard information. Unlike the Vendor Specific options, the information transported is “site” specific and option codes 128-254 are used for encoding.

For Nortel IP Phones, the Voice Gateway Media Card information involves the location of the Voice Gateway Media Card in the network. This varies for different sites and can be implemented in a Site Specific option. If the Vendor Encapsulation option is used, the information is first encoded in a Site

Specific option. Nortel has provided a list of five possible Site Specific option codes to implement the Voice Gateway Media Card information. Only one of the five codes must be configured to carry the information, but the choice is available to offset the possibility that the option code chosen has been used for other purposes.

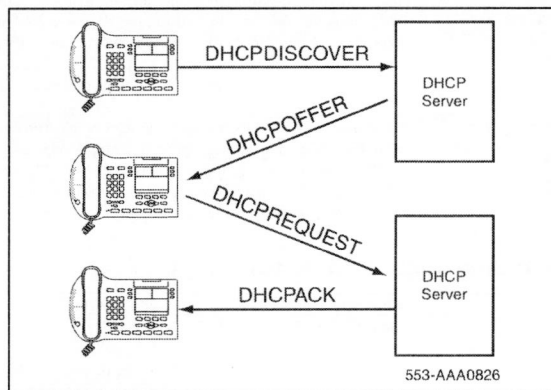
IP acquisition sequence

This section focuses on the mechanics and sequence of the DHCP message exchange as the IP Phone uses DHCP for IP acquisition. Although the IP Phone requests many network configuration parameters as well as an IP address, the following cases focus on the concept of “how” instead of “what” information is acquired. Also, the IP Phone is used as the sample client but the situations apply to other DHCP clients as well.

Case 1

Case 1 is a typical situation where an IP Phone 2004 requests services from a DHCP server. This is shown in Figure 45 on page 285 and explained in the following section.

Figure 45
IP acquisition phase – Case 1



- 1 The IP Phone initiates the sequence by broadcasting a DHCPDISCOVER message.
- 2 A DHCP server on the network sees the broadcast, reads the message, and records the MAC address of the client.
- 3 The DHCP server checks its own IP address pool(s) for an available IP address and broadcasts a DHCPOFFER message if one is available. Usually the server ARPs or PINGs the IP address to make sure it is not being used.
- 4 The IP Phone sees the broadcast and after matching its MAC address with the offer, reads the rest of the message to find out what else is being offered.
- 5 If the offer is acceptable, the IP Phone sends out a DHCPREQUEST message with the DHCP server's IP address in the Server IP address field.
- 6 The DHCP server matches the IP address in the Server IP address field against its own to find out to whom the packet belongs.

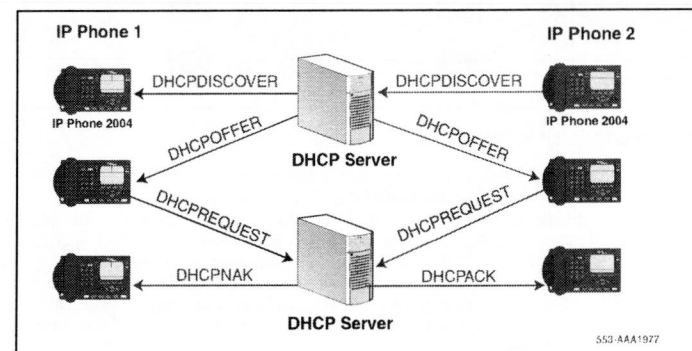
- 7 If the IPs match and there is no problem supplying the requested information, the DHCP server assigns the IP address to the client by sending a DHCPACK.
- 8 If the final offer is not rejected, the IP acquisition sequence is complete.

Case 2

The IP acquisition is unsuccessful if either the server or the client decides not to participate, as follows:

- If the DHCP server cannot supply the requested information, it sends a DHCPNAK message and no IP address is assigned to the client. This can happen if the requested IP address has already been assigned to a different client. See Figure 46.
- If the client decides to reject the final offer (after the server sends a DHCPACK message), the client sends a DHCPDECLINE message to the server, telling the server the offer is rejected. The client must restart the IP acquisition by sending another DHCPDISCOVER message in search of another offer.

Figure 46
IP acquisition sequence – Case 2



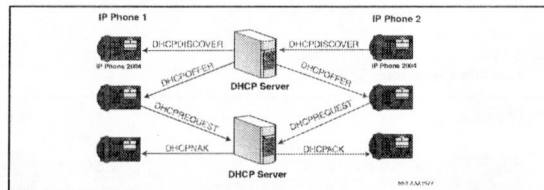
Case 3

Finally, when a client is finished with a particular IP address, it sends a DHCPRELEASE message to the server which reclaims the IP address. If the client requires the same IP address again, it can initiate the process as follows:

- 1 The IP Phone broadcasts a DHCPREQUEST to a particular DHCP server by including the server's IP address in the Server IP Address field of the message. Since it knows the IP address it wants, it requests it in the DHCP message.
- 2 The DHCP server sends a DHCPACK message if all the parameters requested are met.

Case 1 is similar to Case 3, except the first two messages have been eliminated. This reduces the amount of traffic produced on the network. See Figure 47.

Figure 47
IP acquisition sequence – Case 3

**Multiple DHCPOFFERS**

In some networks, if more than one DHCP server is present, a client can receive multiple DHCPOFFER messages. Under these situations, the IP acquisition sequence depends on the client. The client can wait for multiple offers, or accept with the first offer it receives. If it accepts multiple offers, it compares them before choosing one with the most fitting configuration parameters. When a decision is made, the message exchange is the same as if there is only one DHCP server and proceeds as in the previous cases. The servers that were not chosen to provide the service do not participate in the exchange.

For example, the IP Phone 2004 responds only to DHCPOFFERS that have the same unique string identifier, "Nortel-i2004-A", as the IP Phone 2004. This string must appear in the beginning of the list of Voice Gateway Media Card parameters. Without this string, the IP Phone 2004 does not accept the DHCPOFFER, even if all parameters requested and Voice Gateway Media Card information are present. If no valid DHCPOFFERS are sent then, the IP Phone 2004 keeps broadcasting in search of a valid offer.

With multiple DHCP servers on the same network, a problem can occur if any two of the servers have overlapping IP address range and no redundancy. DHCP redundancy is a property of DHCP servers. This redundancy enables different DHCP servers to serve the same IP address ranges simultaneously. Administrators must be aware that not all DHCP servers have this capability.

IP Phone support for DHCP

This section covers the three uses of DHCP (Full, Partial, and VLAN Auto Discovery) by IP Phones 2002, 2004, and 2007.

An "IP Phone 2004-aware" DHCP server is needed only for the Full DHCP and VLAN Auto discovery. An IP Phone can obtain its IP address and subnet mask using Partial DHCP. The "IP Phone 2004 aware" part returns the Node IP and registration port number. In the case of the DHCP Auto Discovery, it returns the VLAN IDs. Separate DHCP vendor-specific entries are needed for the Full DHCP data and the VLAN Auto Discovery data. When using the VLAN Auto Discovery, both Full DHCP and VLAN Auto Discovery must be configured. Full DHCP and Auto VLAN are implemented as separate functions in the IP Phone firmware. However, in practice, Full DHCP and Auto VLAN are frequently used together.

Full DHCP

DHCP support in the IP Phone requires sending a "Class Identifier" option with the value "Nortel-i2004-A" in each DHCP DHCPOFFER and DHCPACK message. Additionally, the telephone checks for either a Vendor Specific option message with a specific, unique to Nortel IP Phone 2004, encapsulated sub-type, or a Site Specific DHCP option.

In either case, an IP Phone 2004-specific option must be returned by the IP Phone 2004 aware DHCP server in all Offer and Acknowledgement (ACK) messages. The IP Phone uses this option's data to configure the information required to connect to the TPS.

The DHCP response is parsed to extract the IP Phone's IP address, subnet mask, and gateway IP address. The vendor specific field is then parsed to extract the Server 1 (minimum) and optionally Server 2. By default, Server 1 is always assumed to be the "primary" server after a DHCP session.

For the IP Phone to accept Offers/Acks, the messages must contain all of the following:

- A router option (needs a default router to function)
- A subnet mask option
- A Vendor Specific option as specified below or a Site Specific option as specified below.
 - The initial DHCP implementation required only the Vendor Specific encapsulated sub-option. In inter-op testing with Windows NT (up to Service Release 4), it was discovered that Windows NT does not properly adhere to RFC 1541. As a result this option is not possible. The implementation was changed to add support for either Vendor Specific sub-ops or Site Specific options. This new extension has been tested and verified to work with Windows NT.
 - The site-specific options are all DHCP options between 128 (0x80) and 254 (0xFE). These options are reserved for site specific use by the DHCP RFCs.

Format for IP Phone 2004 Terminal DHCP Class Identifier Field

All IP Phones (IP Phones 2x and IP Softphone 2050) fill in the Class ID field of the DHCP Discovery and Request messages with the following:

"Nortel-i2004-A", where:

- ASCII encoded, NULL (0x00) terminated
- unique to IP Phone 2004
- "-A" uniquely identifies this version

Format for IP Phone 2004 Terminal DHCP Encapsulated Vendor Specific Field

This sub-option must be encapsulated in a DHCP Vendor Specific Option (refer to RFC 1541 and RFC 1533) and returned by the DHCP server as part of each DHCP OFFER and ACK message in order for the IP Phone to accept these messages as valid.

The IP Phone parses this option's data and use it to configure the information required to connect to the TPS.

Note 1: Either this encapsulated sub-option must be present, or a similarly encoded site-specific option must be sent. See "Format of the Encapsulated Vendor Specific Sub-option field" on page 290. Configure the DHCP server to send one or the other – not both.

Note 2: The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the IP Phone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

Format of the Encapsulated Vendor Specific Sub-option field

The format of the field is as follows:

- **Type (1 octet):** 5 choices are provided (0x80, 0x90, 0x9d, 0xbf, 0xfb [128, 144, 157, 191, 251]), allowing the IP Phone to operate when one or more values is already in use by a different vendor. Select only one TYPE byte.
- **Length (1 octet):** variable – depends on message content.
- **Data (length octets):** ASCII based with the following format:

Nortel-i2004 -A,iii,jjj,kkk,lll:ppppp,aaa,rrr;iii,jjj,kkk,lll:ppppp,aaa,rrr.

The components in this string are described in Table 53 on page 291.

Table 53
Encapsulated Vendor Specific Sub-option field

Parameter	Description
Nortel-i2004-A	Uniquely identifies this as the Nortel option Signifies this version of this specification
iii.jjj.kkk.lll.ppppp	Identifies IP address:port for server (ASCII encoded decimal)
aaa	Identifies Action for server (ASCII encoded decimal, range 0 – 255)
rrr	Identifies retry count for server (ASCII encoded decimal, range 0 – 255). This string can be NULL terminated although the NULL is not required for parsing.
ASCII symbols	The comma “,” is used to separate fields The semicolon “;” is used to separate Primary from Secondary server information The period “.” is used to signal end of structure

Table 54 shows the “pieces” of the Nortel option string. The Nortel designator Nortel-i2004-A is separated from the Connector Server strings using a comma. The Connect Servers are separated using a semi-colon.

Table 54
Nortel option string

Nortel-i2004-A,iii.jjj.kkk.lll.ppppp,aaa,rrr;iii.jjj.kkk.lll.ppppp,aaa,rrr.					
Nortel Class Identifier Field	comma	Primary Connect Server	semicolon	Secondary Connect Server	period
Nortel-i2004-A	,	iii.jjj.kkk.lll.ppppp,aaa,rrr	;	iii.jjj.kkk.lll.ppppp,aaa,rrr	.

Note 1: “aaa” and “rrr” are ASCII encoded decimal numbers with a range of 0–255. They identify the “Action Code” and “Retry Count”, respectively, for the associated TPS server. Internally to IP Phone 2004 they are stored as 1 octet (0x00 – 0xFF). Note that these fields must be no more than 3 digits long.

Note 2: The string enables the configuration of information for two Connect Servers. One Connect Server exists for each IP node. In the typical system configuration of a single IP node, only the primary Connect Server is required. In this case, the primary Connect Server string must be ended with a period (.) instead of a semi-colon (;). For example, “Nortel-i2004-A,iii.jjj.kkk.lll.ppppp,aaa,rrr.”

If the secondary Connect Server portion of the string is specified, then the string information is typically the same as the primary Connect Server information. For example:
“Nortel-i2004-A,iii.jjj.kkk.lll.ppppp,aaa,rrr;iii.jjj.kkk.lll.ppppp,aaa,rrr.”

When the ‘Enhanced Redundancy for IP Line Nodes’ feature is used, two different Connect Server strings can be configured, separated with a semi-colon (;). This enables the telephone to register to two different nodes. For more information about the ‘Enhanced Redundancy for IP Line Nodes’ feature, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

Note 3: Action code values (0–255):
1 — UNISum Hello (currently only this type is a valid choice)
all other values (0, 2–255) — reserved

Note 4: iii.jjj.kkk.lll are ASCII-encoded, decimal numbers representing the IP address of the server. They do not need to be 3 digits long as the “.” and “;” delimiters guarantee parsing. For example, ‘001’, ‘01’, and ‘1’ would all be parsed correctly and interpreted as value 0x01 internal to the IP Phone 2004. Note that these fields must be no more than three digits long each.

Note 5: ppppp is the port number in ASCII encoded decimal. The port number must be set to 4100.

Note 6: In all cases, the ASCII encoded numbers are treated as decimal values and all leading zeros are ignored. More specifically, a leading zero does not change the interpretation of the value to be OCTAL encoded. For example, 0021, 021, and 21 are all parsed and interpreted as decimal 21.

Format for IP Phone 2004 Terminal DHCP Site Specific Option

This option uses the "reserved for site specific use" DHCP options (number 128 to 254 – refer to RFC 1541 and RFC 1533) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone to accept these messages as valid.

The IP Phone pulls the relevant information out of this option and uses it to configure the IP address and so on for the primary and (optionally) secondary TPS's.

Note 1: Either this site specific option must be present or a similarly encoded vendor-specific option must be sent (as previously described). For example, configure the DHCP server to send one or the other – not both.

Note 2: The choice of using either Vendor Specific or Site Specific options is provided to enable Windows NT DHCP servers to be used with the IP Phone. Windows NT servers do not properly implement the Vendor Specific Option and as a result, Windows NT implementations must use the Site Specific version.

Format of the DHCP Site Specific field

The format of the DHCP Site Specific field is the same as the format of the Encapsulated Vendor Specific Sub-option field. Refer to "Format of the Encapsulated Vendor Specific Sub-option field" on page 290.

Partial DHCP

Partial DHCP is the default DHCP response from a DHCP server which has not been configured to provide the Vendor Specific information. Using Partial DHCP, an IP Phone can obtain its IP address, subnet mask, and gateway IP address. The remainder of the configuration information is manually entered at the IP Phone.

DHCP Auto Discovery

DHCP Auto Discovery must be used only if the telephone and PC are:

- connected to the same Layer 2 switch port through a three-port switch
- on separate subnets

The DHCP server can be configured to supply the VLAN information to the IP Phones. The server uses the Site Specific option in the DHCP offer message to convey the VLAN information to the IP Phone.

Configuring a DHCP Server for VLAN Discovery is optional. This configuration is done in addition to any done for Full DHCP configuration and it is required only when configuring the VLAN Auto Discovery.

This method is based on the assumption that the default VLAN will be the data VLAN and the tagged VLAN will be the voice VLAN. Enter the voice VLAN information into the data VLAN and subnet's DHCP server. Enter the standard IP Phone configuration string into the voice VLAN and subnet's DHCP server pool.

The following definition describes the IP Phone 2004-specific, Site Specific option. This option uses the "reserved for Site Specific use" DHCP options (DHCP option values 128 to 254) and must be returned by the DHCP server as part of each DHCP OFFER and DHCPACK message for the IP Phone to accept these messages as valid. The IP Phone extracts the relevant information and uses the information to configure itself.

Format of the field

The format of the field is: Type, Length, Data.

Type (1 octet):

There are five choices:

- 0x80 (128)
- 0x90 (144)
- 0x9d (157)

- 0xbf (191)
- 0xfb (251)

Providing a choice of five types enables the IP Phones to operate if a value is already in use by a different vendor. Select only one Type byte.

Length (1 octet):

This is variable; it depends on message content.

Data (length octets):

ASCII based format: "VLAN-A:XXX+YYY+ZZZ," where,

- "VLAN-A:" – uniquely identifies this as the Nortel DHCP VLAN discovery. Additionally, the "-A" signifies this version of this spec. Future enhancements could use "-B" for example.
- ASCII "+" or "." is used to separate fields.
- ASCII "," is used to signal end of structure.
- XXX, YYY and ZZZ are ASCII encoded decimal numbers with a range of 0-4095. The number is used to identify the VLAN IDs. There are a maximum of 10 VLAN IDs can be configured in the current version. String "none" or "NONE" means no VLAN (default VLAN).

The DHCP OFFER message carrying VLAN information is sent out from the DHCP server without a VLAN tag. However, the switch port adds a VLAN tag to the packet. The packet is untagged at the port of the IP Phone.

Appendix D: Setup and configuration of DHCP servers

Contents

This section contains information on the following topics:

Install a Windows NT 4 or Windows 2000 server	297
Configure a Windows NT 4 server with DHCP	298
Configure a Windows 2000 server with DHCP	301
Install ISC's DHCP Server	307
Configure ISC's DHCP Server	308
Configure ISC's DHCP to work with the IP Phones	308
Example 1: Configuration file	310
Install and configure a Solaris 2 server	312
Install a Solaris 2 Server	312
Configure a Solaris 2 server	312

Install a Windows NT 4 or Windows 2000 server

To set up the Windows NT 4 or Windows 2000 server, follow the instructions provided in the installation booklet. After completion, install the latest Service Pack and make sure the DHCP Manager is included.



WARNING

If installing a Windows NT 4 server with Service Pack 4 or later, follow the installation instructions included with the server hardware.

Configure a Windows NT 4 server with DHCP

Configure a Windows NT 4 server with DHCP services using the DHCP Manager provided. Follow the steps in Procedure 10 to launch the DHCP Manager.

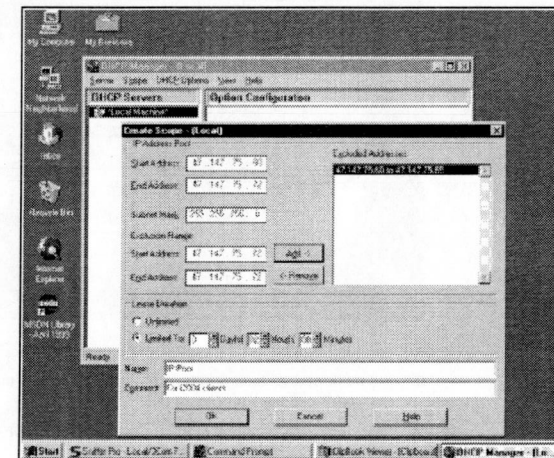
Procedure 10

Launching the DHCP Manager in Windows NT 4

- 1 Click on the Windows **Start** button.
- 2 Select **Programs > Administrative tools (Common) > DHCP Manager**. The **DHCP Manager** window opens.
- 3 Double-click **Local Machines** in the left pane. The **Create Scope - (Local)** window opens. See Figure 48 on page 298.

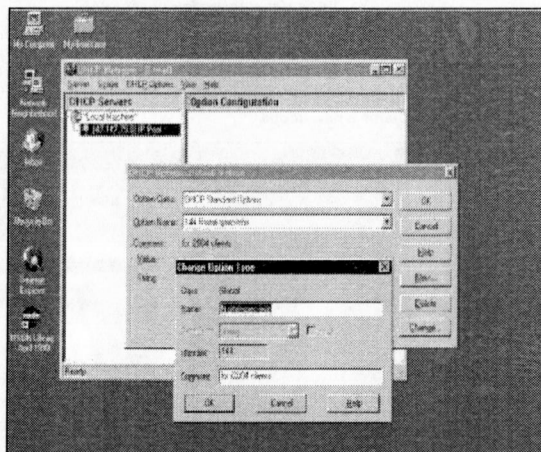
Figure 48

Define a new scope



- 4 Create and then fill in the information. Click **OK** when finished.
- 5 In the **DHCP Manager - (Local)** window, highlight the scope that serves the IP Phones clients.
- 6 From the **DHCP Options** menu, select **Default Values**. The **DHCP Options - Default Values** window opens.
- 7 Click the **New** button. See Figure 49 on page 299. The **Change Option Type** window opens.

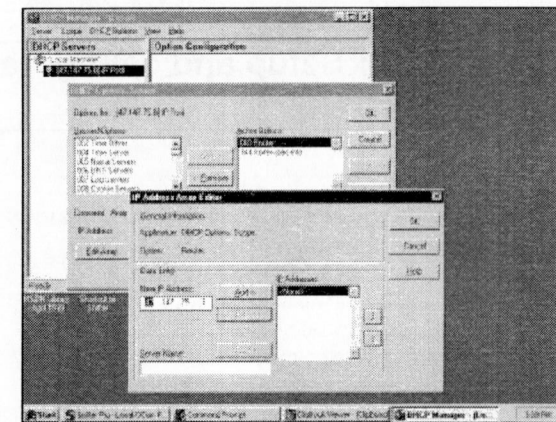
Figure 49
Define the Nortel-specific option



- 8 Fill in the information and click **OK** when finished. Click **OK** again.
- 9 From the **DHCP Manager - (Local)** window, highlight the scope to which the DHCP options are to be added.
- 10 From the **DHCP Options** menu, select **Scope**. The **DHCP Options Scope** window opens.

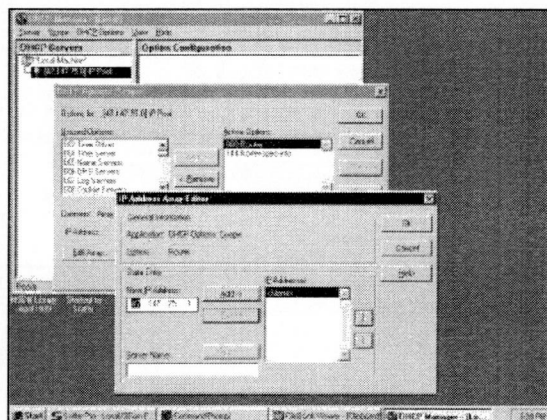
- 11 Choose standard DHCP options from the left panel and click the **Add ->** button to add them to the right panel. See Figure 50 on page 300.

Figure 50
Add standard DHCP options to scope



- 12 Click the **Edit Array** button. The **IP Address Array Editor** window opens. Edit the default value and then click **OK**. Click **OK** again.
- 13 From the **DHCP Manager - (Local)** window, highlight the scope that needs to be activated.
- 14 From the **DHCP Options** menu, select **Scope**. The **DHCP Options Scope** window opens.
- 15 Click on the **Activate** button.
- 16 The light bulb next to the scope should turn yellow. See Figure 51 on page 301.

Figure 51
Activate the scope



Note: If DHCP Auto Discovery needs to be configured, see page 294.

End of Procedure

Configure a Windows 2000 server with DHCP

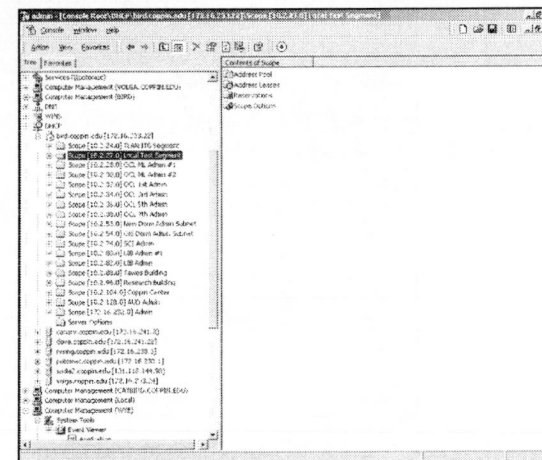
Configure a Windows 2000 server with DHCP services using the DHCP Manager. Follow the steps in Procedure 11.

Procedure 11

Launching the DHCP Manager in Windows 2000

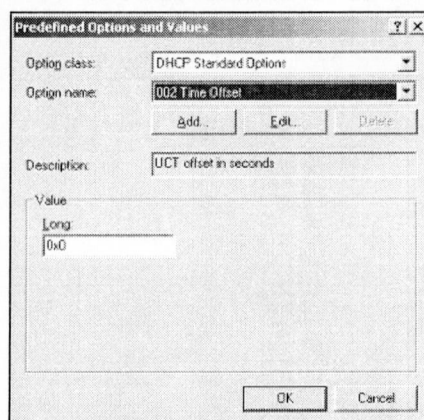
- 1 Click on the Windows **Start** button. Select **Programs > Administrative Tools > DHCP**. The administrative console window opens. See Figure 52 on page 302.

Figure 52
Windows 2000 administration console



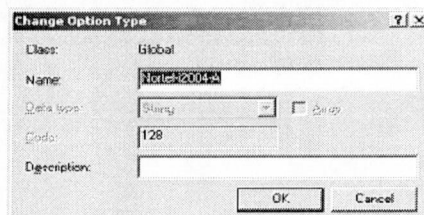
- 2 Highlight DHCP and expand the DHCP option (if it is not already expanded).
- 3 Highlight the server and right-click to open the pop-up menu. Select **Set Predefined Options** from the menu. Do not go into the Vendor Specific settings. The **Predefined Options and Values** window opens. See Figure 53 on page 303.

Figure 53
Predefined Options and Values



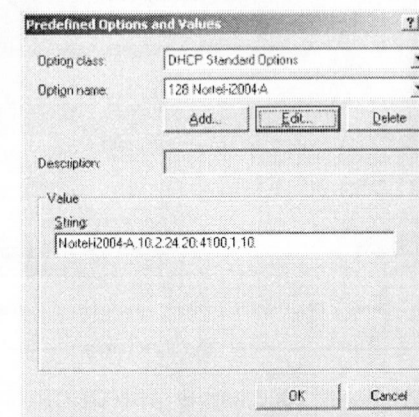
- 4 Click **Add**. The **Change Option Type** window opens. See Figure 54 on page 303.

Figure 54
Change Options Type



- 5 Enter the desired **Name**. For this example, the name of **Nortel-i2004-A** is entered. See Figure 54 on page 303.
- 6 Select **Code 128**.
- 7 Click **OK** to close the window. The **Predefined Options and Values** window reopens with the string **128 Nortel-i2004-A** entered in the **Option name** field. See Figure 55.

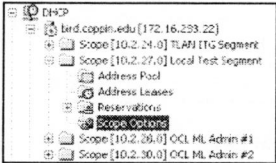
Figure 55
Predefined Options and Values with data entered



- 8 Under the **Value** area, enter the following string in the **String** field: **Nortel-i2004-A,x.x.x.x:4100,1,10**; using the following guidelines:
- The string is case-sensitive.
 - Place a period at the end of the string.
 - Commas are used as separators.
 - Spaces are not allowed.
 - x.x.x.x is the IP address of the IP Telephony node.

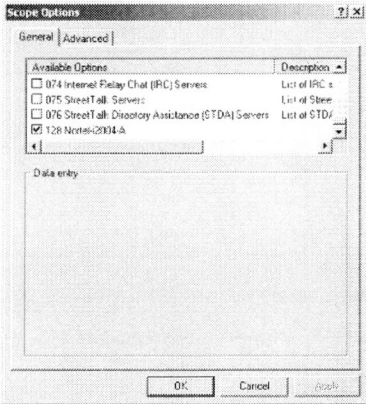
- If it is a BCM, replace the 4100 value with 7000.
- 9 Click **OK**.
- 10 The Option Type must now be added to the applicable scopes. Click on the scope (**Scope [x.x.x.x] name**) to expand the scope, then click **Scope Options**. See Figure 56.

Figure 56
Scope and Scope Options



- 11 The **Scope Options** window opens. See Figure 57 on page 306. On the **General** tab, scroll to the bottom of the list and check the **128 Nortel-i2004-A** option.

Figure 57
Scope Options



- 12 Click **OK**. The Option Name and Value appear in the right pane of the administrative console window. See Figure 58 on page 307.

Procedure 12

Configuring ISC's DHCP server

- 1 Configure the server to identify a client correctly as an IP Phone 2001, IP Phone 2002, IP Phone 2004, or IP Phone 2007. This is done using a **match** statement with a conditional **if** enclosed inside a **class** declaration, as follows:

```
class "i2004-clients"{
    match if option vendor-class-identifier =
    4e:6f:72:74:65:6c:2d:69:32:30:30:34:2d:41:00;}

```

The Hex string represents the text string "Nortel-i2004-A". If the vendor-class-identifier obtained from the client's DHCPDISCOVER message match this Hex-encoded string, then the server adds this client to the "i2004-clients" class. Once a client is classified as a member of a class, it must follow the rules of the class.

- 2 Declare a pool of IP addresses exclusively for the members of the "i2004-clients" class. The pool declaration is used to group a range of IP addresses together with options and parameters that apply only to the pool.
- 3 Restrict access to the pool. Use the **allow** or **deny** statement to include or exclude the members of a particular class. For example, the follow configuration code enables only members of "i2004-clients" to use this IP address pool:

```
pool{
    allow members of "i2004-clients";
    range 47.147.75.60 47.147.75.65;
    option routers 47.147.75.1;

    # Nortel special string
    option vendor-encapsulated-options
    80:3d:4e:6f:72:...;}

```

Note: If a client is not a member of this class, it is not assigned an IP address from this pool, even if there were no other available IP addresses.

- 4 The DHCP OFFER from the ISC server must include the Voice Gateway Media Card information if the client is an IP Phone 2001, IP Phone 2002, IP Phone 2004, or IP Phone 2007. There are two methods to encode the necessary information for the IP Phone 2004 client:

- a. Use the **vendor-encapsulated-options** option (as in the previous example) to encode the information as a sub option.
- b. Define a **Site Specific option** to carry the necessary information. To define a site specific option:

- give a declaration in the form of the name of the option, the option code, and the type of data it carries outside any pool or network declarations. For example:

option Nortel-specific-info code 144 = string;

- replace the vendor-encapsulated option inside the pool statement with the definition,

option Nortel-specific-info = "Nortel ...";

Note: If DHCP Auto Discovery needs to be configured, see page 294.

End of Procedure

Example 1: Configuration file

The following format must be used for encoding the Voice Gateway Media Card information. In addition to the configuration statements provided, other network and subnet declarations must also be included in the configuration file. As mentioned in the beginning of this section, read the man files and use the following example as a guideline:

```
# File name: dhcpd.conf
# Location: /etc/
# Description: Configuration file for ISC dhcpd server

# Author: Cecilia Mok
# Date: September 24, 1999

# Global option definitions common for all supported
# networks...

default-lease-time 300;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 255.255.255.255;
```



```
# Defining Nortel-specific option for IP Phone 2004 client
option my-vendor-specific-info code 144 = string;

# Declaring a class for IP Phones type 2002, 2004, and 2007
# clients.
# Add new clients to the class if their Class Identifier
# match the special IP Phone 2004 ID string.
class "i2004-clients"
{
    match if option vendor-class-identifier =
        4e:6f:72:74:65:6c:2d:69:32:30:30:34:2d:41:00;
}

# Declaring another class for PC clients
class "pc-clients"
{}

# Declaring a shared network
# This is to accommodate two different subnets on the same
# physical network; see dhcpd.conf.man5 for more details

shared-network "myNetwork"
{
    # Declaring subnet for current server
    subnet 47.147.77.0 netmask 255.255.255.0
    {}

    # Declaring subnet for DHCP clients
    subnet 47.147.75.0 netmask 255.255.255.0
    {
        # Pool addresses for i2004 clients
        pool
        {
            allow members of "i2004-clients";
            range 47.147.75.60 47.147.75.65;

            option routers 47.147.75.1;

            # Nortel special string
            option Nortel-specific-info = "Nortel...";
        }

        default-lease-time 180;
        max-lease-time 300;
    }
}
```

Finally, before starting the server, create a blank dhcpd.leases file in the /etc/ directory, which is the same location as the dhcpd.conf file. To start the server, go to /var/usr/sbin/ and type:

```
./dhcpd
```

To run in debug mode, type:

```
./dhcpd -d -f
```

Install and configure a Solaris 2 server

Install a Solaris 2 Server

To set up the Solaris 2 server, consult the accompanying manual and online documentation.

Configure a Solaris 2 server

Follow the steps in Procedure 13 on page 312 to configure Solaris 2 with DHCP.

Procedure 13 Configuring a Solaris 2 server

1 Read the following man pages:

- dhcpconfig
- dhcptab
- in.dhcpd

Note: There are also directions at the end of each page referring to other sources that are helpful.

2 Collect information about the network such as subnet mask, router/Media Gateway and DNS server IP addresses as specified. Make sure this information is current.

- 3 Log on as **root** and invoke the interface by typing **dhcpcconfig** at the prompt. A list of questions is presented and the administrator must supply answers that are then used to configure the DHCP server.

Note: Solaris 2 uses a text-based interface for configuring DHCP services.

Note: If DHCP Auto Discovery needs to be configured, see page 294.

End of Procedure

Procedure 14
Configuring Solaris 2 to work with IP Phones

- 1 Do one of the following:
- Create a symbol definition for defining a Site Specific option by typing the following in the dhcptab configuration table located at /etc/default/dhcp:


```
NI2004 s Site,128,ASCII,1,0
```
 - Use the dhtadm configuration table management utility by typing the following command at the prompt:


```
dhtadm -A -s NI2004 -d 'Site,128,ASCII,1,0'
```

 where:
 - NI2004: symbol name
 - s: identify definition as symbol
 - Site: site specific option
 - 128: option code
 - ASCII: data type
 - 1: granularity
 - 0: no maximum size of granularity, that is, infinite
- 2 Create a Client Identifier macro by doing one of the following:
- entering the following:


```
Nortel-i2004-A m:NI2004="Nortel...":
```
 - Use the dhtadm command:


```
dhtadm -A -m Nortel-i2004-A -d ':NI2004="Nortel...":'
```

- 3 Invoke the DHCP services on the Solaris server by entering at the prompt.:

in.dhcpd,

Specify **-d** and/or **-v** options for debug mode. See man page in.dhcpd for more details.

End of Procedure

An example of the tables used in this project is as follows:

DhcptabTable

```
Locale      m      :UTCoffst=18000:
nbvws286    m
:Include=Locale:LeaseTim=150:LeaseNeg:DNSdmain=ca.nortel.com:/
DNSserv=47.108.128.216 47.211.192.8 47.80.12.69:
47.147.75.0  m      :NISdmain=bvwlabs:NISservs=47.147.64.91:
47.147.64.0  m
:Broadcast=47.147.79.255:Subnet=255.255.240.0:MTU=1500:/

Router=47.147.64.1:NISdmain=bvwlabs:NISservs=47.147.64.91:
#
NI2004      s      Site,128,ASCII,1,0
Nortel-i2004-A m
:NI2004="Nortel-i2004-A,47.147.75.31:4100,1,5;47.147.77.143:4100,1,5":
```

Network Table

```
01006038760290 00 47.147.65.198 47.147.74.36 944600968
nbvws286
0100C04F662B6F 00 47.147.65.199 47.147.74.36 944600959 nbvws286
```

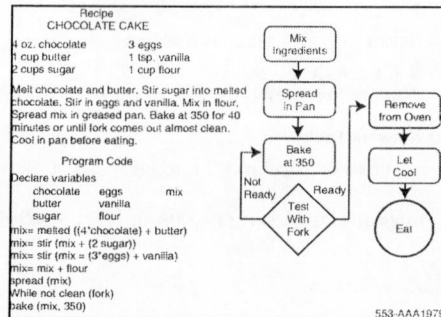
List of terms

Algorithm

A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. Algorithms can be expressed in any language, from natural languages like English or French to programming languages like FORTRAN.

We use algorithms every day. For example, a recipe for baking a cake is an algorithm (see Figure 59). Most programs, with the exception of some artificial intelligence applications, consist of algorithms. Inventing elegant algorithms – algorithms that are simple and require the fewest steps possible – is one of the principal challenges in programming.

Figure 59
Chocolate cake recipe



ATM

Short for **Asynchronous Transfer Mode**, a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

Current implementations of ATM support data transfer rates of from 25 to 622 Mbps (megabits per second). This compares to a maximum of 100 Mbps for Ethernet, the current technology used for most LANs.

Some people think that ATM holds the answer to the Internet bandwidth problem, but others are skeptical. ATM creates a fixed channel, or route, between two points whenever data transfer begins. This differs from TCP/IP, in which messages are divided into packets and each packet can take a different route from source to destination. This difference makes it easier to track and bill data usage across an ATM network, but it makes it less adaptable to sudden surges in network traffic.

When purchasing ATM service, there generally is a choice of four different types of service:

- Constant Bit Rate (CBR) specifies a fixed bit rate so that data is sent at a constant rate. This is analogous to a leased line.
- Variable Bit Rate (VBR) provides a specified throughput capacity but data is not sent evenly. This is a popular choice for voice and video conferencing data.
- Unspecified Bit Rate (UBR) does not guarantee any throughput levels. This is used for applications, such as file transfer, that can tolerate delays.
- Available Bit Rate (ABR) provides a guaranteed minimum capacity but allows data to be burst at higher capacities when the network is free.

CBR

Constant Bit Rate. See ATM.

CIR

Committed Information Rate. A Frame relay term. CIR is the level of data traffic in bits that a carrier agrees to handle – not at all times, but averaged over a period of time.

Client

The client part of a client-server architecture. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables a user to send and receive e-mail.

COPS-PR

Common Open Policy Service (COPS) is an IETF standard (RFC 2748). It provides a standard protocol for exchange of policy information between network servers, and network clients such as routers and switches. COPS-PR (COPS Usage for Policy Provisioning) is a provisioning layer designed to facilitate the implementation of new policies, as defined by Policy Information Bases (PIBs).

Network administrators can quickly deploy new services and configurations across a network, using the COPS-PR layer, to dynamically update network devices with new policies. It provides the necessary services to propagate DiffServ policy information across the network.

DiffServ

Differentiated Services. DiffServ specifies, on a per-packet basis, how IP traffic is handled. The handling is specified based on the packet's DiffServ CodePoint (DSCP). A method for adding Quality of Service (QoS) to IP networks from the IETF, DiffServ is the preferred Layer 3 QoS mechanism for CS 1000 Release 4.5.

Operating at Layer 3 only, DiffServ uses the IP Type Of Service (TOS) field as the DiffServ byte (DS byte).

DiffServ domain

A network segment that is DiffServ-aware.

DiffServ edge

Where the DiffServ domain begins. Defined in the DiffServ Architecture RFC 2475.

DiffServ Edge Node

The first Layer 3-aware device that a packet encounters.

DSCP

DiffServ CodePoint. Six bits in an IP packet header that specify how a packet is to be handled on an IP network.

DSP

Digital Signal Processing, which refers to manipulating analog information, such as sound or photographs that has been converted into a digital form. DSP also implies the use of a data compression technique.

When used as a noun, DSP stands for Digital Signal Processor, a special type of coprocessor designed for performing the mathematics involved in DSP. Most DSPs are programmable, which means that they can be used for manipulating different types of information, including sound, images, and video.

Full-duplex

Transmission in both directions at the same time can occur on the bandwidth. The full bandwidth of the link is available in either direction.

Gateway

In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, allow users on different e-mail systems to exchange messages.

H.323

A standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks. In theory, H.323 should enable users to participate in the same conference even though they are using different video conferencing applications. Although most video conferencing vendors have announced that their products will conform to H.323, it's too early to say whether such adherence will actually result in interoperability.

Half-duplex

Packets are transmitted in only one direction at a time. The send and receive bandwidth is shared. Packet collisions can occur on half-duplex links.

IEEE 802 standards
IEEE

Institute of Electrical and Electronics Engineers, pronounced I-triple-E. Founded in 1884 as the AIEE, the IEEE was formed in 1963 when AIEE merged with IRE. IEEE is an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry. In particular, the IEEE 802 standards for local-area networks are widely followed.

802 standards

A set of network standards developed by the IEEE. They include:

- IEEE 802.1: Standards related to network management.
- IEEE 802.2: General standard for the data link layer in the OSI Reference Model. The IEEE divides this layer into two sublayers -- the logical link control (LLC) layer and the media access control (MAC) layer. The MAC layer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5.
- IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD. This is the basis of the Ethernet standard.
- IEEE 802.4: Defines the MAC layer for bus networks that use a token-passing mechanism (token bus networks).
- IEEE 802.5: Defines the MAC layer for token-ring networks.
- IEEE 802.6: Standard for Metropolitan Area Networks (MANs).

IEEE 802.1: network management

Refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- Security: Ensuring that the network is protected from unauthorized users.
- Performance: Eliminating bottlenecks in the network.
- Reliability: Making sure the network is available to users and responding to hardware and software malfunctions.

IEEE 802.1p

The Class of Service bits within an IEEE 802.1Q VLAN tag.

IEEE 802.1Q

The IEEE specification referring to Virtual Local Area Networks (VLANs). It includes "Class of Service" and VLAN ID.

IEEE 802.2: MAC Layer

The Media Access Control Layer is one of two sublayers that make up the Data Link Layer of the OSI model. The MAC layer is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

See a breakdown of the seven OSI layers in the Quick Reference section of Webopedia.

The MAC sublayer uses MAC protocols to ensure that signals sent from different stations across the same channel don't collide.

Different protocols are used for different shared networks, such as Ethernet, Token Ring, and Token Bus.

IP

Abbreviation of **Internet Protocol**, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

The current version of IP is IPv4. A new version, called IPv6 or IPng, is under development.

IPSec

A group of IP security measures. It defines privacy, integrity, authentication, security key management, and tunnelling methods. A secure version of IP, IPSec enables a secure VPN over the Internet, providing optional authentication and encryption at the packet level.

Layer 2 switching

Packets are forwarded based on the destination's MAC address. The switch automatically determines which switch port must be used to send the packet, based on the destination's MAC address. The MAC address location was determined from incoming packets from that MAC address received on that port.

Layer 3 switching

Packet traffic is grouped based on source and destination addresses. The first packet in a flow is routed by a software-based algorithm. Subsequent packets with the same source and destination addresses are switched based on the destination's MAC address (hardware mechanism). This is similar to multi-layer routing and routers with hardware assist.

MIB

Management Information Base. A database of network performance information that is stored on a Network Agent. It contains characteristics and parameters about network devices such as NICs, hubs, switches, and routers. This information is accessed by software like SNMP.

MID

Message Identifier.

MUA

Mail User Agent. The mail program used by an end-user computer to create and read e-mail messages.

NAT

Network Address Translation. It is defined as an Internet standard that lets a LAN use both internal and external IP addresses. This protects an internal IP address from being accessed from outside. NAT translates the internal IP addresses to unique IP addresses before sending out packets. NAT is practical when only a few users in a domain need to communicate outside of the domain at the same time.

Object Identifier

Also known as OID. An object is identified as a numeric value that represents some aspect of a managed device. An Object Identifier (OID) is a sequence of numbers, separated by periods, which uniquely defines the object within an MIB.

OID

See **Object Identifier**.

Policy

A set of rules defining how certain network traffic should be treated. The rules consist of classification, marking, and queuing specifications.

Proxy Server

A server that sits between a client application, such as a web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

Proxy servers have two main purposes:

- **Improve Performance:** Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time. Consider the case where both user X and user Y access the World Wide Web through a proxy server. First user X requests a certain webpage, which we'll call Page 1. Sometime later, user Y requests the same page. Instead of forwarding the request to the web server where Page 1 resides, which can be a time-consuming operation, the proxy server simply returns the Page 1 that it already fetched for user X. Since the proxy server is often on the same network as the user, this is a much faster operation. Real proxy servers support hundreds or thousands of users. The major online services such as CompuServe and America Online, for example, employ an array of proxy servers.
- **Filter Requests:** Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of websites.

PSTN

Short for Public Switched Telephone Network, which refers to the international telephone system based on copper wires carrying analog voice data. This is in contrast to newer telephone networks based on digital technologies, such as ISDN and FDDI.

Telephone service carried by the PSTN is often called plain old telephone service (POTS).

PVC

Permanent Virtual Circuit. All transmitted data between two points follows a pre-determined path.

QoS

Quality of Service. A networking term that specifies a guaranteed throughput level. One of the biggest advantages of ATM over competing technologies such as Frame Relay and Fast Ethernet, is that it supports QoS levels. This allows ATM providers to guarantee to their customers that end-to-end delay does not exceed a specified level.

RMON

Remote Monitoring specification. It is a set of SNMP-based MIBs (Management Information Bases) that define the monitoring, instrumenting, and diagnosis of LANS. It occurs at OSI Layer 2 (DLL). RMON-2 monitors above Layer 2, and can see across segments and through routers. See "SNMP" on page 324.

routing

The process of selecting the correct path for packets transmitted between IP networks by using software-based algorithms. Each packet is processed by the algorithm to determine its destination.

RTP

Real-time Transport Protocol. An IETF standard that supports transport of real-time data, like voice and video, over packet switched networks. It does not provide QoS control.

Server

A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems, however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

Shared-media hub

A central connecting device in a network that joins communication lines together in a star configuration. Packets received on a shared-media hub are transmitted out of all other ports on the hub. This means all links must be half-duplex.

SNMP

Simple Network Management Protocol. A set of protocols for managing complex networks. The first versions of SNMP were developed in the early 1980s. SNMP works by sending messages, called Protocol Data Units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SNMP 1 reports only whether a device is functioning properly. The industry has attempted to define a new set of protocols called SNMP 2 that would provide additional information, but the standardization efforts have not been successful. Instead, network managers have turned to a related technology called RMON that provides more detailed information about network usage.

Subnet

Subnetwork. A segment of an IP network. Packets must be routed in and out of a subnet.

TDM

Time Division Multiplexing, a type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel.

Within T-Carrier systems, such as T-1 and T-3, TDM combines Pulse Code Modulated (PCM) streams created for each conversation or data stream.

UDP

User Datagram Protocol. Part of the TCP/IP protocol suite. It allows for the exchange of datagrams without acknowledgement or guarantee of delivery. UDP is at Layer 4 of the OSI model.

VLAN

Virtual LAN. A logical grouping of network devices, located on different physical LAN segments, into a single domain. This allows the devices to interwork as though they were on the same segment.

WAN

Wide Area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Nortel Communication Server 1000
**Converging the Data Network
with VoIP**

Copyright © 2006 Nortel Networks. All rights reserved.
The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Nortel, Nortel (Logo), the Globemark, SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

Publication number: 553-3001-160
Document release: Standard 5.00
Date: July 2006

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

Produced in Canada

NORTEL